Release Notes for VPN Client, Release 4.0.3

CCO Date: October 1, 2003

Part Number 78-16121-01

Note You can find the most current documentation for the VPN Client at http://www.cisco.com or http://cco.cisco.com. These electronic documents may contain updates and changes made after the hard copy documents were printed.

These release notes support VPN Client software Release 4.0, Release 4.0.1, Release 4.0.2, Release 4.0.2.A, Release 4.0.2.B, and Release 4.03. These release notes describe new features, limitations and restrictions, interoperability notes, caveats, and related documentation. Please read the release notes carefully prior to installation. The section, "Usage Notes," describes interoperability considerations and other issues you should be aware of when installing and using the VPN Client.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Introduction

The VPN Client is an application that runs on a Microsoft® Windows®-based PC, a Sun ultraSPARC workstations, a Linux desktop, or a Macintosh (Mac) personal computer that meets the system requirements stated in the next section. In this document, the term “PC” applies generically to all these computers, unless specified otherwise.

The VPN Client on a remote PC, communicating with a Cisco VPN device at an enterprise or service provider, creates a secure connection over the Internet that lets you access a private network as if you were an on-site user. This secure connection is a Virtual Private Network (VPN).

System Requirements

Refer to Chapter 2, "Installing the VPN Client," in the *VPN Client User Guide for Windows, Release 4.0* or *Cisco VPN Client User Guide for Mac OS X*, as appropriate for your platform, for a complete list of system requirements and installation instructions.

- To install the VPN Client on *any* system, you need
  - CD-ROM drive (if you are installing from CD-ROM)
  - Administrator privileges
- The following table indicates the system requirements to install the VPN Client on each of the supported platforms.

Computer	Operating System	Requirements
Computer with a Pentium®-class processor or greater	• Microsoft® Windows® 98 or Windows 98 (second edition) • Windows ME • Windows NT® 4.0 (with Service Pack 6, or higher) • Windows 2000 • Windows XP	• Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.) • 50 MB hard disk space. • RAM: – 32 MB for Windows 98 – 64 MB for Windows NT and Windows ME – 64 MB for Windows 2000 (128 MB recommended) – 128 MB for Windows XP (256 MB recommended)
Computer with and Intel x86 processor	RedHat Version 6.2 or later Linux (Intel), or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later **Note** The VPN Client does not support Linux kernel Version 2.5.	• 32 MB Ram • 50 MB hard disk space
Sun UltraSPARC computer	32-bit or 64-bit Solaris kernel OS Version 2.6 or later	• 32 MB Ram • 50 MB hard disk space
Macintosh computer	OS X, Version 10.1.0 or later	50 MB hard disk space

The VPN Client supports the following Cisco VPN devices:

- Cisco VPN 3000 Concentrator Series, Version 3.0 and later.
- Cisco PIX Firewall, Version 6.2.2(122) or Version 6.3(1).
- Cisco IOS Routers, Version 12.2(8)T and later

If you are using Internet Explorer, use version 5.0, Service Pack 2 or higher.

Installation Notes

Because of platform differences, the installation instructions for Windows and non-Windows platforms also differ.

- Refer to the *VPN Client User Guide for Windows, Release 4.0*, Chapter 2, for complete installation instructions for Windows users.
- Refer to the *Cisco VPN Client user Guide for Mac OS X*, Chapter 2, for complete installation information for those platforms.

The following notes are important for users who are upgrading to Windows XP and users who want to downgrade to an earlier version of the VPN Client software.

Installing Release 4.0.3

Release 4.0.3 on Windows operating systems is localized for Canadian French and Japanese, as well as English. The following sections describe how to install this version on a Windows system.

Overriding the MSI Installation Language.

To perform this action you must already have Windows Installer Version 2.0 installed. You can determine which version you have by executing msiexec.exe without parameters. If the version is lower than 2.0, execute instmsiw.exe, which updates the software to the correct version.

Note You must run the following commands from the command line, and the current directory must be the install source.

The default installation is in English. To specify a language other than English, enter the following command, *all on the same line*:

```
msiexec /i vpnclient_setup.msi
TRANSFORMS=vpnclient_<language>.mst;vpnclient_help_<language>.mst
```

The supported language codes are:

- fc (Canadian French)

- jp (Japanese)

To force an English only language install, enter the following command:

```
msiexec /i vpnclient_setup.msi
```

To force a Canadian French language installation, enter the following command, *all on the same line*:

```
msiexec /i vpnclient_setup.msi TRANSFORMS=vpnclient_fc.mst;vpnclient_help_fc.mst
```

To force a Japanese language installation, enter the following command, *all on the same line*:

```
msiexec /i vpnclient_setup.msi TRANSFORMS=vpnclient_jp.mst;vpnclient_help_jp.mst
```

Overriding IS Installation Language:

The install image must contain a vpnclient.ini file with the following two lines:

```
[main]
ClientLanguage=<language code>
```

The supported language codes are

- fc (Canadian French)
- jp (Japanese)

Non-localized Features

The following parts of the VPN Client are not localized:

- VPN Client GUI Splash Screen
- Copyright statements
- Log Messages
- Any text pushed down from the VPN 3000 Concentrator. This includes the banner and the user authentication request text message (which most often appears as “Enter User Name and Password”).
- InstallShield text. We are localizing only the MSI install text.
- The company name, “Cisco Systems”, and product name, “VPN Client”.

Installation Notes - Windows Platforms

In addition to the installation considerations for Release 4.0.3, Release 4.0.x includes the following installation considerations for Windows users:

Installing the VPN Client Software Using InstallShield

Installing the VPN Client software on Windows NT, Windows 2000, or Windows XP with InstallShield requires Administrator privileges. If you do not have Administrator privileges, you must have someone who has Administrator privileges install the product for you.

Installing the VPN Client Software Using the MSI Installer

If you are using the MSI installer, you must have Windows NT-based products such as Windows NT 4.0 (with SP6), Windows 2000, or Windows XP. Installing with MSI also requires Administrator privileges.

Note Windows Installer 2.0 must be installed on a Windows NT or Windows 2000 PC before configuring the PC for a Restricted User with Elevated Privileges (CSCea37900).

VPN Client Installation Using Windows Installer (MSI) Requires Windows NT SP6

When you attempt to install the VPN Client using MSI install (vpnclient_en.exe) on NT SP3, SP4, or SP5, the error messages do not indicate that the VPN Client cannot be installed on those operating systems because they are unsupported. Once the errors occur, no other messages are displayed and the installation is aborted.

When you attempt to run vpnclient_en.exe on Windows NT SP3, SP4, or SP5 you see the following messages:

“Cannot find the file instmsiw.exe (or one of its components). Make sure the path and filename are correct and that all the required libraries are available.”

-then-

"Cannot find the file MSIEXEC (or one of its components). Make sure the path and filename are correct and that all the required libraries are available."

The Windows Installer (MSI) can be installed only on NT SP6, so the error messages you see using earlier service packs are due to an MSI incompatibility (CSCdy05049).

Installation Notes - Solaris Platforms

The following sections describe actions you must take when installing the VPN Client on a Solaris platform.

Uninstall an Older VPN Client If Present on a Solaris Platform

If you have a previous version of the VPN Client running under Solaris, you *must* uninstall the older VPN Client before installing a new VPN Client. You are not required to uninstall an old VPN Client, if one is present, *before* installing a new VPN Client for Linux or Mac OS X.

Refer to the *Cisco VPN Client User Guide for Linux, Solaris, and Mac OS X*, Chapter 2, for complete uninstallation information.

Disable the ipfilter Firewall Kernel Module Before Installing the VPN Client on a Solaris Platform

If you have an IP firewall installed on your workstation, the reboot after installation of the VPN Client takes an inordinate amount of time. This is caused by a conflict between the vpnclient kernel module cipsec and the ipfilter firewall module. To work around this issue, disable the ipfilter firewall kernel module before you install the VPN Client (CSCdw27781).

Using the VPN Client

- To use the VPN Client, you need
  - Direct network connection (cable or DSL modem and network adapter/interface card), or
  - Internal or external modem, and

- To connect using a digital certificate for authentication, you need a digital certificate signed by one of the following Certificate Authorities (CAs) installed on your PC:
  - Baltimore Technologies (www.baltimoretechnologies.com)
  - Entrust Technologies (www.entrust.com)
  - Netscape (www.netscape.com)
  - Verisign, Inc. (www.verisign.com)
  - Microsoft Certificate Services — Windows 2000
  - A digital certificate stored on a smart card. The VPN Client supports smart cards via the MS CAPI Interface.

New Features in Release 4.0

Release 4.0 of the VPN Client software includes the following new features.

Virtual Adapter

A virtual adapter is a software-only driver that acts as a valid interface in the system. Its purpose is to solve protocol incompatibility problems. The virtual adapter appears in the network properties list just like a physical adapter.

Note When installing the Release 4.0 VPN Client on a Windows 2000 system, the following warning appears during the virtual adapter installation, indicating that no digital signature was found and asking whether to continue the installation:

```
The Microsoft digital signature affirms that software has been tested
with Windows and that the software has not been altered since it was
tested.

The software you are about to install does not have a Microsoft digital
signature. Therefore, there is no guarantee that this software works
correctly with Windows.

Cisco Systems VPN Adapter
```

If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.

Do you want to continue the installation?

If you see this message, click "Yes" to continue (CSCdz14583).

Common Graphical Interface for Windows and Mac VPN Clients

In Release 4.0, the VPN Client provides a consistent graphical user interface across all supported Windows operating systems and Mac OS X, recognizing that the Windows and Mac operating systems follow different conventions, and that the Windows version has additional features. The VPN Client documentation is based on this new user interface.

Alerts (Delete With Reason)

In Release 4.0, the VPN Client can display to the user the reason for a VPN 3000 Concentrator-initiated disconnection. If the VPN 3000 Concentrator, Release 4.0, disconnects the VPN Client and tears down the tunnel, the VPN Client, Release 4.0, displays a popup window showing the reason for the disconnect and also logs a message to the Notifications log and the IPSec log file. For IPSec deletes that do not tear down the connection, the event message appears only in the log file.

The administrator on the VPN 3000 Concentrator can enable or disable this feature, called Alerts in the VPN Concentrator configuration. It is not configurable on the VPN Client. When this feature is enabled, the VPN 3000 Concentrator and the VPN Client negotiate whether to display these messages. See the *Cisco VPN Client User Guide, Release 4.0*, for a description of the conditions that can cause such disconnects.

Single IPSec-SA

Rather than creating a host-to-network security association (SA) pair for each split-tunneling network, this feature provides a host-to-ALL approach, creating one tunnel for all appropriate network traffic apart from whether split-tunneling is in use. With this feature, the VPN Client supports a single SA per VPN connection and directs all the appropriate traffic through this tunnel, regardless of whether split tunneling is in use. The Statistics page on the VPN Client reflects the traffic for this single SA.

Personal Firewall Enhancements

In Release 4.0, the VPN Client supports Sygate Personal Firewall and Sygate Personal Firewall Pro, Version 5.0, Build 1175 and higher. Other supported features new with this release include:

- The ability to enable or disable stateful firewalls from the command line.
- Configurable ICMP permissions.

Coexistence with Third-Party VPN Vendors

In Release 4.0, the VPN Client is compatible with VPN clients from Microsoft, Nortel, Checkpoint, Intel, and others. This feature offers the ability to use other VPN products while the Cisco VPN Client is installed.

Improved RADIUS SDI XAuth Request Handling

The VPN Client, Release 4.0, includes improvements in RADIUS SDI XAuth handling, which may improve performance. Administrators can configure this feature in the .pcf file and the .ini file. For information, see *VPN Client Administrator Guide, Release 4.0*, Chapter 2.

New, ISO-Standard Format for Log File Names

The format of the names of log files generated by the VPN Client GUI has changed to LOG-yyyy-MM-dd-hh-mm-ss.txt from MMM-d-yyyy-hh-mm-ss.log. This new format complies with the ISO 8601 extended specification for representations of dates and times and avoids issues with localization.

The new log file names have a chronological order that is the same as their alphanumeric order. This provides for a method of enumerating only the log files generated by the GUI.

Enhancements to GINA

Release 4.0.2 includes an improved application launch verification mechanism employed by the Graphical Identification and Authentication (GINA) dynamic-link library (DLL). This affects only the Windows NT4, Windows 2000, and Windows XP platforms (CSCeb12179).

Usage Notes

This section lists issues to consider before installing Release 4.0.2 of the VPN Client software.

In addition, you should be aware of the open caveats regarding this release. Refer to “Open Caveats” on page 31 of these Release Notes for the list of known problems.

Potential Application Compatibility Issues

You might encounter the following compatibility issues when using the VPN Client with specific applications. Whenever possible, this list describes the circumstances under which an issue might occur and workarounds for potential problems.

Windows Interoperability Issues

The following known issues might occur with the indicated Microsoft Windows operating systems and applications software.

WINS Support

On Windows 95 and Windows 98, dynamic WINS support works with DHCP-enabled adapters (for example, PPP or NIC adapters that get their IP information dynamically). For static configurations, users must manually configure the adapters with WINS information.

Windows NT

Users running Windows NT 4.0 with Service Pack 4 require a hot fix from Microsoft for proper operation. This fix is available on the Microsoft GetHostByName API Returns Unbindable Address page: http://support.microsoft.com/support/kb/articles/Q217/0/01.ASP.

Importing a Microsoft Certificate Using Windows NT SP3

The following problem has occurred on some Windows NT SP3 systems (CSCdt11315**)**.

When using the Client with digital certificates stored in the Microsoft certificate store, the Client may fail to connect. This is accompanied by the following Client event in the Log Viewer:

4101 13:41:48.557 01/05/01 Sev=Warning/2 CERT/0xA3600002
Could not load certificate (null) from the store.

Workaround: Two workarounds exist. Choose one of the following:

- Import the certificate from the Microsoft certificate store into the Cisco certificate store using the Cisco Certificate Manager. Refer to “Importing a Certificate” in the *VPN Client User Guide for Windows, Release 4.0*, Chapter 6.
- Alternatively, upgrade to a Windows Service Pack later than SP3.

VPN Client Cannot Launch Microsoft Connection Manager

The VPN Client does not see a dialup connection made with Microsoft Connection Manager because of incompatibilities between the requirements of the two applications (CSCdx85663).

Windows 98 Might Hang on Shutdown

On some Windows 98 PCs with the VPN Client installed, if you restart the PC, it may stop responding (that is, "hang") on the screen that says "Windows is shutting down".

Wait a minute. If the PC is still not responding, press the reset button. When the PC reboots, it should not run through ScanDisk, indicating the shutdown was successful in closing all open files. This problem may occur on some PCs and not on others, and we are looking for a solution. Windows 98 shutdown has numerous issues, as can be seen the following Microsoft Knowledge Base Article:

"Q238096 - How to Troubleshoot Windows 98 Second Edition Shutdown Problems" (CSCdt00729).

Windows 2000 (only) Requires Adding Client for MS Networks for Dialup Connections

For the Cisco VPN Client running on a Windows 2000 system, you cannot access Microsoft resources unless you add the Client for Microsoft Networks for the Dial-up adapter.

Aladdin Runtime Environment (RTE) Issue with Windows NT and Windows 2000

Using versions of the Aladdin Runtime Environment (RTE) on Windows NT and Windows 2000 can cause the following behavior. The login prompt that is posted by the Aladdin etoken when connecting the VPN Client can get hidden in the background. If this happens, the VPN connection can timeout and fail with the following event:

"System Error: Connection Manager failed to respond."

A side effect of this is that the VPN Client's service and dialer might become out of synch, and the PC might need to be restarted (CSCdv47999). To avoid this issue, use the Aladdin Runtime Environment (RTE) version 2.65 or later.

Microsoft MSN Installation

Microsoft's MSN installation fails if you have already installed the VPN Client. Uninstall the VPN Client before you install MSN. After MSN has completed installation, you can install the VPN Client.

WINS Information Might Not Be Removed from Windows Servers If Not Disconnected Before Shutdown

If the VPN Concentrator is configured to send WINS server addresses down to the VPN Client and the PC is shut down or restarted without first disconnecting the VPN Client, the WINS servers are not removed from the network properties. This might cause local PC registration and name resolution problems while not connected with VPN.

To work around this problem, do *one* of the following:

- Be sure to disconnect the VPN Client before shutting down. If you are having problems, check your network properties and remove the WINS entries if they are not correct for your network.
- Alternatively, enable "Disconnect VPN connection when logging off". Go to Options > Windows Logon Properties, check Disconnect VPN connection when logging off (CSCdv65165).

VPN Client May Falsely Trigger Auto Initiation Connection Event though the NIC Card Has Been Removed

The 4.0 VPN Client with Auto Initiation enabled on a Windows NT system may exhibit the following behavior. After removing a NIC card, the VPN Client may continue to trigger an Auto Initiation connection event though the NIC card has been removed. To stop its connection attempts, you can place the VPN Client in Suspended mode after a failed or canceled VPN connection. You can also disable this feature from the GUI by using Options > Automatic VPN Initiation, and unchecking "Enable". If you add a new NIC, the problem goes away. (CSCdx46812).

DNS

For DNS resolution, if the DOMAIN NAME is not configured on the network interface, you need to enter the fully qualified domain name of the host that needs to be resolved.

Network Interfaces

- The VPN Client cannot establish tunnels over Token Ring. However, it does not conflict with an installed Token Ring interface.
- DELL Docking Station users running the VPN Client on Windows NT may experience bluescreen failures if the latest version of Softex Docking Services has not been installed. The Softex Docking Service utilities are available directly from the DELL Support Web site, http://search.dell.com/index.asp. Select the checkbox for the File Library and search for the term “Softex Docking Services”.

Network ICE BlackICE Defender Configuration

Network ICE's BlackICE Defender is a traffic monitoring security product. If you properly configure it, BlackICE Defender can work with the VPN Client. You must configure BlackICE Defender for Trusting, Nervous, or Cautious mode. If you use Nervous or Cautious mode, add the public IP address of the VPN Concentrator to the list of trusted addresses. You can now configure the VPN Client to work with BlackICE Defender configured for Paranoid mode when in Tunnel-everything mode. Split Tunneling requires BlackICE to be in Trusting, Nervous, or Cautious mode.

The Cisco VPN Client firewall has the following requirements for BlackICE (BlackICE Defender 2.5 or greater or BlackICE Agent 2.5 or greater). For BlackICE Defender 2.5, copy the BICTRL.DLL file from the Cisco installation release medium to the BlackICE installation directory on the VPN Client PC. This is a mandatory step for making a connection requiring BlackICE.

BlackICE Defender version 2.9 and greater includes the BICTRL.DLL file in the Network ICE distribution medium, so that you do not need to copy it from the Cisco installation release medium.

Microsoft Outlook Error Occurs on Connection or Disconnect

The following Microsoft Outlook error might occur when the VPN Client connects or disconnects:

“Either there is no default mail client, or the current mail client cannot fulfill the messaging request. Run Microsoft Outlook and set it as the default mail client.”

This message does not affect operation of the VPN Client. The issue occurs when Microsoft Outlook is installed but not configured for email, although it is the default mail client. It is caused by a Registry Key that is set when the user installs Outlook.

To eliminate this message, do one of the following:

- Right-click the Outlook icon, go to Properties, and configure it to use Microsoft Exchange or Internet Mail as the default mail client.
- Use Internet Explorer to configure the system to have no default mail client.
- Configure Outlook as the default mail client (CSCdv67594).

Adjusting the Maximum Transmission Unit (MTU) Value - Windows Only

VPN Encapsulation adds to the overall message length. To avoid refragmentation of packets, the VPN Client must reduce the MTU settings. The default MTU adjusted value is 1300 for all adapters. If the default adjustments are not sufficient, you may experience problems sending and receiving data. To avoid fragmented packets, you can change the MTU size, usually to a lower value than the default. To change the MTU size, use the VPN Client SetMTU utility. If you are using PPPoE, you may also have to set the MTU in other locations. Refer to the following table for the specific procedures for each type of connection.

The MTU is the largest number of bytes a frame can carry, not counting the frame's header and trailer. A frame is a single unit of transportation on the Data Link Layer. It consists of header data, plus data that was passed down from the Network Layer, plus (sometimes) trailer data. An Ethernet frame has an MTU of 1500 bytes, but the actual size of the frame can be up to 1526 bytes (22-byte header, 4-byte CRC trailer).

Recognizing a Potential MTU Problem

If you can connect with the Cisco VPN Client but cannot send or receive data, this is likely an MTU problem. Common failure indications include the following:

- You can receive data, such as mail, but not send it.
- You can send small messages (about 10 lines), but larger ones time out.
- You cannot send attachments in email.

Setting the MTU Value

If you are *not* experiencing a problem, do *not* change the MTU value. Usually, an MTU value of 1300 works. If it doesn't, the end user must decrease the value until the Cisco VPN Client passes data. Decrement the MaxFrameSize value by 50 or 100 until it works.

The following table shows how to set the MTU value for each type of connection.

Connection Type	Procedure
Physical Adapters	Use the SetMTU utility supplied with the Cisco VPN Client.
Dial-up	Use the SetMTU utility supplied with the Cisco VPN Client.
PPPoE - All Vendors	**Windows XP *only*** Use SetMTU
PPPoE - EnterNet	**Windows 98** • On the main desktop, right click on My Network Places and go to Properties. The Network window opens. • Double-click the Network TeleSystems PPPoE Adapter. • On the Network TeleSystems window, click the Advanced tab, and then click MaxFrameSize. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.
	Windows 2000 • On the main desktop, right-click My Network Places and go to Properties. The Network and Dial-Up Connections window opens. • Right-click and go to Properties on each connection until you find the connection that has the NTS EnterNet PPPoE Adapter. • Once you find the correct connection, click Configure on the right side of the window. • On the next window, click the Advanced tab, then click MaxFrameSize. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.

Connection Type	Procedure
PPPoE - WinPoet	**Windows 98:** WinPoet does not provide user control over the PPPoE MTU under Windows 98. **Windows 2000** WinPoet does not provide a user interface to control the MTU size, but you can control it by explicitly setting the following registry key: HKLM/system/currentcontrolset/control/class/<guid>/<adapternumber> adapter(000x): Value: MaxFrameSize Value type: DWORD Data: 1300 (or less) The GUID and adapter number can vary on different systems. Browse through the registry, looking for the MaxFrameSize value (CSCdu80463). **Caution** Edit the registry only if you are comfortable doing so. Incorrect registry entries can make your PC unstable or unusable.
PPPoE - RasPPPoE	**Windows 98** • On the main desktop, right-click My Network Places and go to Properties. The Network window opens. • Find the PPP over Ethernet Protocol that is bound to the Network card that is in your PC, then double click on it. • In the General Tab check Override Maximum Transfer Unit. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.
	Windows 2000 • On the main desktop, right-click My Network Places and go to properties. The Network and Dial-Up Connections window opens. • Right-click the connection the PPPoE Protocol was installed to, and go to properties. • When the window opens, double-click PPP over Ethernet Protocol. • In the General Tab, check Override Maximum Transfer Unit. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.

Asante FR3004 Cable/DSL Routers Require Asante Firmware Version 2.15 or Later

Versions of the Asante firmware caused a problem with rekeying and keepalives when a VPN Client had an all-or-nothing connection to a VPN Concentrator through an Asante FR3004 Cable/DSL router. Version 2.15 (or later) of the Asante firmware resolves these issues. For more information about Asante cable/DSL routers, see the following Web sites:

- http://www.asante.com/products/routers/index.html
- http://www.practicallynetworked.com/pg/router_guide_index.asp

Using Nexland Cable/DSL Routers for Multiple Client Connections

All Nexland Pro routers support passing multiple IPSec sessions through to Cisco VPN 3000 Series Concentrators. To enable this function, the Nexland user must select IPSec Type 2SPI-C on the Nexland options page.

The discontinued Nexland ISB2LAN product correctly handles a single connection, but problems can occur when attempting to make multiple client connections to the same Secure Gateway from behind an ISB2LAN Nexland Cable/DSL router. Nexland has fixed this problem in the Nexland Pro series of routers (CSCdt10266).

Cert DN Matching Cannot Match on Email Field EA

You cannot match on the Cert DN field (EA) when using the Peer Cert DN Verification feature because the VPN Concentrator does not assign a value to that field (CSCdx25994).

VPN Dialer Application Can Load During OS Shutdown or Restart

When using the VPN Client's Start Before Logon feature (Windows NT, Windows 2000, or Windows XP) in "fallback" mode, the VPN dialer application loads during a shutdown or restart of the operating system. This will not cause any problems and can be ignored (CSCdu02071).

America Online Users (AOL) Versions 5.0 and 6.0

The VPN Client supports AOL Version 5.0. AOL Version 6.0 is also supported, with one limitation: when connected, browsing in the network neighborhood is not available.

America Online Users (AOL) Version 7.0

AOL Version 7.0 uses a proprietary heartbeat polling of connected clients. This requires the use of split tunneling to support the polling mechanism. Without split tunneling, AOL disconnects after a period of time between 5 and 30 minutes.

AOL 7 Disconnects after VPN Authentication

When making a dialup connection with AOL 7.0 Revision 4114.537 (for Windows 95, 98, ME, Windows 2000 and XP), then attempting to connect with the VPN Client, AOL might disconnect while the user is being authenticated. This is an AOL issue, not a VPN Client problem (CSCdy45351).

VPN Client Fails to Connect over Some AOL Dialup Connections

The Cisco VPN Client connecting over an AOL dialup connection fails to complete the connection, particularly when using AOL 7.0 and 8.0

The AOL dialup process uses a fallback method which, if your initial attempt to connect fails, resorts to a different connection type for the second attempt. This second attempt can sometimes cause AOL to communicate over two PPP adapters (visible in ipconfig /all output). When this happens, the VPN Client cannot connect. This is a known issue, and AOL is investigating the problem.

The workaround is to try to reconnect the dialup connection to try to avoid getting two PPP adapters (CSCea29056).

Browser Interoperability Issues

The following known issues might occur when using the VPN Client with the indicated browser software.

Issues Loading Digital Certificate from Microsoft Certificate Store on Windows NT SP5 and on IE 4.0 SP2

The following error occurs in the VPN Client log when using a Digital Certificate from the Microsoft Certificate Store. This can occur on Windows NT 4.0 with Service Pack 5 and on Internet Explorer 4.0 with SP2 and using the VPN Client v3.1 or v3.5:

"Could not load certificate cn=Joe Smith,ou=Engineering,o=MyCompany,l=Buffalo, st=new york,c=US,e=jsmith@mycompany.com from the Unsupported Store store"

Both the VPN Client and the Certificate Manager can see and validate the Certificate, but when you try to connect using that Certificate, you get a message in the Connection History dialog that says, "Failed to establish a secure connection to the security gateway".

To fix this problem, do *one* of the following:

- Upgrade to Internet Explorer v5.0 or greater.
- Upgrade the PC to Service Pack 6.0a (CSCdv70215).

Requirements for using VPN Client for Windows Using Digital Certificate With Non-exportable Keys

To use certificates with non-exportable keys, you must have the VPN Client, Release 3.6 or 4.0, and your PC must have Internet Explorer version 5.0 SP2 or later installed to function properly. (CSCdx90228).

Entrust Entelligence Issues

The following known issues might occur when using Entrust Entelligence software with the VPN Client.

Potential Connection Delay

Using the VPN Client with Entrust Entelligence might result in a delay of approximately 30 seconds if you are trying to connect while Entrust is "online" with the CA. This delay varies, depending on your Entrust CA configuration. If the Entrust CA is on the private network, then the chance of Entrust being online are low, since the VPN connection is needed to communicate with the CA.

If you experience this delay, do *one* of the following:

- Wait for the delay to end and proceed with the VPN connection normally.

- Before initiating the VPN Client connection, log out of Entrust. The VPN Client will initiate the Entrust Login Interface with the “work offline” checkbox checked, which alleviates the problem. The easiest way to log out of Entrust is to right-click on the Entrust tray icon (gold key) and select “Log out of Entrust” (CSCdu25495).

Entrust System Tray Icon Might Erroneously Indicate Logout

When using VPN Client with Start Before Logon (Windows NT and 2000) and Entrust Entelligence, the Entrust system tray icon indicates that it is “logged out” once in Windows. It is really logged in, just not in the normal Windows desktop. The reason for this is that the context that Entrust was logged into was on the “Logon desktop”. This is an Entrust issue, not a VPN Client problem.

Entrust operates normally once logged into within Windows (CSCdu29239).

Entrust Client May Appear Offline

After establishing a VPN connection with Entrust Entelligence certificates, the Entrust client may appear offline. It may appear this way even after the Entrust client has successfully communicated with the Entrust i500 directory.

To work around this issue, do *one* of the following:

- Upgrade to Entrust Entelligence version 5.1 SP3 or later.
- Once connected, right click on the Entrust tray icon (gold key) and uncheck “Work Offline”. This manually puts Entrust online (CSCdu33638).

Use Entrust Entelligence 4.0 with VPN Client Release 3.5.1 or 3.1 Start Before Logon

When using the Release 3.5.1 or 3.1 VPN Client with the Entrust Entelligence 4.0 software, the Start Before Logon feature does not function properly. Upgrading to Entrust Entelligence 5.1 resolves this problem (CSCdu61926).

Some Entrust Dialogs Do Not Display Properly When Using VPN Client Start Before Logon

When using the VPN Client with Start Before Logon and Entrust Entelligence, some Entrust dialogs do not display properly on the logon desktop that displays before going into Windows NT or Windows 2000. The first time the VPN Client dialer and service access the Entrust certificates, it prompts for a security check. This prompt displays in Windows, but not at the logon screen.

To work around this problem, connect the VPN Client once, while in Windows and after installing, to register the VPN applications (ipsecdialer.exe and cvpnd.exe) with Entrust. Once you have done this you can use it at the logon desktop (CSCdu62212).

Renewing Entrust Entelligence Certificate (Key Update) Requires Entrust Version 5.1 SP 3 or Later

Entrust Entelligence certificate renewal (key update) will not work over a VPN Client connection unless Entrust Entelligence version 5.1 SP3 or later is being used. Other Entrust Entelligence operations using older versions work properly.

To work around this issue, do *one* of the following:

- Upgrade to Entrust Entelligence version 5.1 SP3 or later.
- Computers need to have Entrust digital certificates renewed by placing them directly on the network during the renewal period to get updated (CSCdu84038).

Accessing Online Glossary Requires Connection to Cisco.com

The Glossary button at the top of all Help screens tries to contact univercd at www.cisco.com (the Cisco documentation site). This connection requires connectivity to Cisco's main web site. If your PC does not have a corporate Internet connection or your firewall blocks access, the following error appears when you attempt to access the Glossary:

"The page cannot be displayed."

To access the Glossary, you must be connected to www.cisco.com (CSCdy14238).

ZoneAlarm Plus Versions 3.1.274 and Earlier Are Incompatible with VPN Client

The following known incompatibility exists between the Cisco VPN Client and Zone Labs ZoneAlarm Plus version 3.1.274 and earlier. If you are using such a version of ZoneAlarm Plus, please visit http://www.zonelabs.com or contact your Zone Labs representative for an update.

On a PC with ZoneAlarm Plus version 3.1.274 (or earlier) and the VPN Client, the following errors occur when the PC boots:

On Windows 2000:

ZAPLUS.exe has generated errors and will be closed by Windows. You will need to restart the program.

An error log is being generated.

The Application Log states:

The application, ZAPLUS.EXE, generated an application error. The error occurred on 7/23/2002... The exception was c0000005 at address 00401881 (<nosymbols>).

Similar errors occur on other Windows operating systems.

The result of this error is that the ZoneAlarm GUI does not run, and therefore a user can not change any settings in ZoneAlarm Plus or allow new programs to access the Internet.(CSCdy16607).

ZoneLabs Automatically Adds Loopback and VPN 3000 Concentrator Addresses to Trusted Zone for Windows NT PCs

The Loopback address and the VPN 3000 Concentrator's address are automatically added to the ZoneLabs "Trusted Zone" on Windows NT-based systems.

If a Windows NT based-PC has ZoneAlarm, ZoneAlarm Pro, or Zone Labs Integrity Agent, and the VPN Client Release 4.0 installed on it, the loopback address (127.0.0.1) is automatically added to Zone Labs "Trusted Zone" when the Client service is started. Additionally, the VPN 3000 Concentrator's address is automatically added to the "Trusted Zone" when a connection is made (CSCea61272).

Harmless Warning Might Occur with Linux Kernel 2.4

Linux users running 2.4 kernels may encounter the following warning when the VPN Client kernel module is loaded:

Warning: loading /lib/modules/2.4.18-3/CiscoVPN/cisco_ipsec will taint the kernel: no license

This message indicates that the VPN Client kernel module is not licensed under the GPL, so the Linux kernel developers will not debug any kernel problems that occur while this kernel module is loaded. This message does not affect the operation of the VPN Client in any way (CSCdy31826).

DHCP Route Renewal in Windows 2000 and Windows XP

In a Windows 2000 or Windows XP environment, if the public network matches the private network (for example, a public IP address of 192.168.1.5, with a subnet mask of 255.255.0.0, and an identical private IP address) and the public network's route metric is 1, then traffic might not be tunneled to the private network (CSCdz88896). The same problem can occur if you are using a virtual adapter and the public metric is smaller than the virtual adapter metric.

In Windows 2000 and Windows XP, you can increase the metric of the public network by doing the following steps:

Step 1 Select Start > Settings > Control Panel > Network and Dial-up Connections.

Step 2 Select the public interface and click properties for the public interface.

Step 3 Select Internet Protocol (TCP/IP) and get the properties for the Internet Protocol (TCP/IP).

Step 4 Click Advanced, and set the interface metric to 2 or greater.

Solaris Client Using Routed RIP Might Lose Connectivity

If the VPN Client running in the Solaris environment uses routed RIP to learn its default route, you might lose connectivity. This is because RIP is blocked when the VPN Client is connected in all tunneling mode (CSCdv75825).

Data Meant for Private Network Stays Local if VPN Client's Local Network Is on Same IP Subnet as Remote Private Network

This problem occurs only with the VPN Client, Release 4.0 and only with Virtual Adapter (Windows 2000 and Windows XP), when the VPN Client's local network is on the same IP subnet as the remote private network. When a VPN connection is up, data meant for the private network stays local. For example: 192.168.1.0/255.255.255.0

The VPN Client, Release 4.0, with Virtual Adapter attempts to modify local route metrics to allow data to pass over the VPN tunnel. In some cases, it is impossible for the VPN Client to make this modification (CSCdz38680).

To work around this problem, make the change manually, using the following procedure:

Step 1 Run > Control Panel > Network and Dialup Connections.

Step 2 Right-click on the adapter in question and select Properties.

Step 3 From the Adapter Properties dialog, select TCP/IP from the list and click Properties.

Step 4 Click Advanced and increase the number in the "Interface metric" box by 1 (it is usually 1, so making it 2 works).

Step 5 Click OK to exit out of all dialogs.

Step 6 The VPN connection should now work.

VPN Client Supports Sygate Personal Firewall V. 5.0, Build 1175

The supported version of Sygate Personal Firewall is version 5.0, build 1175. Earlier versions might cause the following Blue screen to occur on a Windows NT-based system that has made many connects/disconnects with the VPN Client (CSCdy62426):

Stop: 000000d1 (BAD0B0B8, 00000002, 00000000, BFF12392)

Driver_IRQL_Not_Less_Or_Equal

***Address BFF12392 base at BFF10000, Datestamp 3CCDEC2C - Teefer.sys

The 4.0 VPN Client Is Not Supported on Windows 95

The VPN Client for Windows, Release 4.0, requires the use of the Windows 98 or later operating system. We recommend updating your Operating system to a newer version of Windows (CSCea06231).

VPN Client Not Supported on Windows NT Servers

The VPN Client is not supported on any Windows NT server version (including Windows 2000 and Windows XP/.NET/2003 servers). Only Windows NT 4.0 Workstation and Windows 2000 Workstation are the supported platforms.

No Limit to Size of Log File

When logging is enabled on the VPN Client, all of the log files are placed in the Program Files\Cisco Systems\VPN Client\logs directory and are date and time stamped. There is no limit to the size of the log when logging is enabled. The file will continue to grow in size until logging is disabled or the VPN Client program is closed. The log is still available for viewing until the VPN Client program is re-launched, at which time the display on the log tab and log window are cleared (CSCdy87504). The log file remains on the system and a new log file is created when the VPN Client, with logging enabled, is launched.

Start Before Logon and Microsoft Certificate with Private Key Protect Fails

Trying to connect the VPN client using Start Before Logon (SBL) and Microsoft Machine-based certificates fails. This is a Microsoft issue, not a VPN Client problem.

If your certificate has private key protection enabled, every time you use the certificate keys you are either prompted for a password to access the key, or notified with a dialog and asked to click OK.

The prompt displayed when using a certificate with private key protection appears on the Windows Desktop. You do not see this message while at the “Logon” desktop, therefore the VPN Client cannot gain the access to the certificate needed to connect.

Use *one* of the following workarounds:

- Get a certificate without private key protection (just make sure it is machine-based, otherwise it won't be accessible before logging on).
- Instead of using Start Before Logon, log on to the PC using cached credentials, make the VPN connection, and— using the “stay connected at logoff” feature—logoff/logon with the VPN established to complete the domain logon (CSCea03349).

Downgrading VPN Client from Release 4.0 Causes Start Before Logon Failure

Start Before Logon fails if the VPN Client is downgraded from Release 4.0 to 3.6. The reason for this is that the file csgina.dll is upgraded when the VPN Client version 4.0 is installed. If the VPN Client is downgraded to version 3.6, the csgina.dll file for version 4.0 is not replaced, and this breaks ability in the VPN Client version 3.6 to Start Before Logon (CSCea03685).

Follow this procedure to drop back to the VPN Client version 3.6 from version 4.0.

Step 1 Uninstall the VPN Client version 4.0.

Step 2 After rebooting, search for csgina.dll. This file is found in the System32 directory.

Step 3 Rename csgina.dll to something like csgina.old.

Step 4 Install the VPN Client version 3.6.

Linksys Wireless AP Cable/DSL Router Version 1.44 or Higher Firmware Requirement

To use the VPN Client behind a Linksys Wireless AP Cable/DSL router model BEFW11S4, the Linksys router must be running version 1.44 or higher firmware. The VPN Client cannot connect when located behind a Linksys Wireless AP Cable/DSL router model BEFW11S4 running version 1.42.7 firmware. The VPN Client may see the prompt for username/password, then it disappears (CSCdz52156).

Faultlog.txt File Logs Severity 1 Events

The faultlog.txt file is created when severity 1 events occur. It logs only severity 1 events. All severity 1 log messages go to the logs and also to faultlog.txt. This file exists in the installation directory of the VPN Client.

The advantage that the faultlog.txt file provides is that messages are logged even when the log viewer is not running. For example, errors during service initialization can't be logged to the log viewer, because these errors happen even before the service has attached itself to the log viewer.

Certificates exported from Netscape 7 do not import into the VPN Client Macintosh Version

This incompatibility exists with Netscape 7.0 and the Release 3.7.x Macintosh versions of the VPN Client. Netscape 7.0 uses the latest RSA libraries that are not compatible with the previous RSA libraries that the Clients are using. Previous versions of Netscape are still compatible with the VPN Client.

To work around this issue, export the certificate using a browser other than Netscape 7.

On the Mac OS X platform, Internet Explorer 5.2 that comes installed does not allow certificates to be exported. The best course of action for these users is to either enroll and export the certificate from a Windows workstation and email it to the Mac user or to use direct enrollment from the Client itself.

Verisign works fine with the Macintosh version of the VPN Client. But the "browsers" available on the Macintosh don't export certificates (Verisign or others) in the proper format for the VPN Client to receive them, or they don't allow the export of certificates at all (IE). This is because IE is a Windows product and doesn't support on the Macintosh platform everything the normal Windows IE does (CSCdz23397).

Open Caveats

Caveats describe unexpected behavior or defects in Cisco software releases. The following lists are sorted by platform and then by identifier number for the specified platform.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II on CCO, choose Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

This section lists open caveats for the VPN Client running on a Windows platform.

- CSCdt07491

  The VPN Client may swap Primary and Secondary WINS received from the Concentrator. In a few cases, the VPN Client receives a Primary and a Secondary WINS server from the Concentrator but swaps them when they are added to the IP Configuration. If this happens, it may cause browsing problems if the Secondary WINS server is not as populated as the Primary. Disconnecting and reconnecting may fix the problem.

- CSCdt07673

  When the VPN Client is installed on a Windows 2000 PC with the Efficient Networks NTS EnterNet 300 PPPoE version 1.41 or 1.5c, the following message appears:

  "EnterNet could not find the (adapter) for complete pc management NIC (adapter). But it did locate the (adapter) for complete pc management NIC (adapter) - Deterministic Network Enhancer Miniport adapter through which your network server is reachable. Do you want to switch to this adapter?"

Answer Yes every time this question appears. The installation then continues normally.

A similar message appears on Windows NT 4.0. The message is:

"EnterNet could not find the (adapter). But it did locate the (adapter) through which your network server is reachable. Do you want to switch? Yes No"

Answer Yes to this question. The installation then continues normally.

If the VPN Client is uninstalled, the next time the NTS EnterNet 300 PPPoE version 1.41 is used the message, "EnterNet could not find the (adapter). But it did locate the (adapter) through which your network server is reachable. Do you want to switch? Yes No"

Answer Yes to this question. The installation then continues normally.

- CSCdt07787

  Problems have occurred when an ISA legacy NIC card (IBM Etherjet 10MB) is used in a PC with PnP OS enabled. The WINS servers did not function correctly when a VPN Client connection was made. This could be an issue with other legacy NIC cards as well.

  The end results are that the WINS servers sent from the Secure Gateway cannot be viewed in the Network configuration, and problems with browsing/logon over the VPN connection may occur.

  Workaround:

  Disable PnP OS in the PC's BIOS or statically configure the WINS servers.

- CSCdt13380

  When you connect the VPN Client to a VPN 3000 Concentrator that issues two DNS servers, both appear under ipconfig /all, but only one appears under the Network settings TCP/IP Properties. DNS server appears to be missing under TCP/IP Properties (Advanced button, DNS TAB). We do not know whether this causes any problems.

- CSCdt41308

  On Windows 98, Windows ME, and Windows NT machines, you may see a problem with FTP file transfers over a long period of time (hours) while connected with the VPN Client. The symptom is that the FTP session never starts (no response to the 'open' command) and the Client Log Viewer shows the following events:

74 22:31:08.704 02/08/01 Sev=Warning/2 IPSEC/0xE370000C
Failed to acquire a TCP control resource, the queue is empty.

75 22:31:08.704 02/08/01 Sev=Warning/2 IPSEC/0xA370001A
VRS processing failed, discarding packet

Other applications like PING and HTTP should work fine, but for FTP to work again, you must disconnect and reconnect the VPN Client.

This problem does not occur on Windows 2000 and Windows NT machines.

- CSCdt56343

  You might see the following problem on systems running Windows NT and Windows 2000 when you are using the Start Before Logon feature of the VPN Client with third-party dialer. If the third-party dialer does not get set to the foreground when launched, add the following parameter to the vpnclient.ini file in the VPN Client directory (\Program Files\Cisco Systems\VPN Client\Profiles):

  [main]
  TopMostDelay=2500

  The value is the time in milliseconds that the VPN Client waits for the third party dialer to load before attempting to place it in the foreground. The default time is 1000 milliseconds.

  Workaround:

  For problem dialers/applications, try 2500 milliseconds or greater.

- CSCdu22174

  SCEP enrollment might fail to complete successfully after the PKI administrator has granted your request.

  Workaround:

  If this happens, delete your failed request and submit a new one.

  To delete the request, click the Certificate tab, select the failed request, and click Delete on the toolbar. Alternatively, open the Certificates menu and select Delete.

- CSCdu50445

  The following issue can exist when using the VPN Client Start Before Logon feature with Entrust SignOn. Entrust SignOn is an add-on to the Entrust Entelligence client that allows logging into the Entrust profile and the NT domain from a single login.

The Entrust SignOn GINA dll does not support chaining to other GINA dll files. To make the Entrust SignOn product and the VPN Client with Start Before Logon function properly together, install the VPN Client after Entrust SignOn. The VPN Client replaces the Entrust GINA (etabcgin.dll) with its own (csgina.dll).

- CSCdu62275

  VPN Client and Entrust Entelligence - VPN Connection timeout.

  In version 3.1, the potential exists for the VPN Client Connection Manager and the VPN dialer to get out of sync with each other. This occurs only after a VPN Client upgrade on the first time the VPN Client accesses a given Entrust profile. The following sequence outlines how a user could get the connection into this state:

Step 1 In the VPN dialer, the user clicks Connect.

Step 2 Entrust prompts for password and security hash check. The user clicks Yes.

Step 3 Entrust prompts for password for cvpnd.exe security access.

If the user waits here or walks away from PC, the VPN Connection times out in 3 minutes.

Step 4 The user returns and enters the Entrust password, then clicks Yes to the security hash check question.

Step 5 The VPN connection completes, and data can be passed. The VPN dialer appears as not connected.

Step 6 Clicking Connect returns “A connection already exists”. The user clicks Cancel, and the dialer appears connected in the system tray.

The VPN connection can be used as a normal connection.

- CSCdu70660

  This issue occurs on a Windows NT PC that is running ZoneAlarm or Sygate Personal Firewall, if the VPN Client is set to Start Before Logon and an upgrade to the VPN Client is implemented. Do not attempt a connection before the logon when you reboot, because both firewalls do not automatically give the VPN Client permission to access the Internet. Both firewalls see the upgrade as a new application attempting to access the Internet, and it requires user permission through its pop-up menus. The user

must logon to the Windows NT PC using cached credentials, then launch a VPN connection. The firewall then asks permission to allow the VPN Client to connect. Answer yes to each connection. After that, Start Before Logon works fine.

- CSCdu77405

  The message, “The necessary VPN sub-system is not available. You will not be able to make a connection to the remote IPSec server.” might appear on a PC when Start Before Logon is enabled on the Client and ZoneAlarm is also running. The message appears when the ctrl+alt+del key combination is pressed. This has happened because the Cisco Systems VPN Service has terminated unexpectedly.

  Workaround:

  Logon to the PC with cached credentials, open “Services” in control panel and start the VPN service. A connection to the VPN Concentrator will be possible once the service has started.

- CSCdu81905

  When connecting to a VPN 3000 Concentrator over PPPoE using the EnterNet 300 client software from Efficient Networks, Inc., if a firewall is required by the VPN Concentrator, the following message might appear:

  “The Client did not match any of the Concentrator's firewall configurations...”

  If this message appears, click OK and then click Connect. The connection to the VPN Concentrator then proceeds successfully.

- CSCdu83054

  If you make connections from the command line interface, the following problem can occur. When a firewall is required to connect and the firewall fails or is shut down, you do not see any message giving the reason for the lost connection.

- CSCdu86399

  If you use the VPN Client with a Digital Certificate and your Client sits behind a Cable/DSL router or some other NAT device, you might not be able to connect to your VPN Gateway device (that is, the VPN 3000 Concentrator). The problem is not with the VPN Client or the Gateway; it is with the Cable/DSL router. When the VPN Client uses a Digital Certificate, it sends the Certificate to the VPN Gateway. Most of the time, the packet with

the Certificate is too big for a standard Ethernet frame (1500), so it is fragmented. Many Cable/DSL routers do not transmit fragmented packets, so the connection negotiation fails (IKE negotiation).

This problem might *not* occur if the Digital Certificate you are using is small enough, but this is only in rare cases. This fragmentation problem happens with the D-Link DI-704 and many other Cable/DSL routers on the market. We have been in contact with a few of these vendors to try to resolve the issue.

Testing with the VPN Client Release 3.1 indicates that VPN Client connections using Digital Certificates *can* be made using the following Cable/DSL routers with the following firmware:

Linksys BEFSRxx v1.39 or v1.40.1

SMC 7004BR Barricade R1.93e

Nexland Pro400 V1 Rel 3M

NetGear RT314 V3.24(CA.0)

Asante FR3004 V2.15 or later

Others like 3COM 3C510, and D-Link DI-704 either had updated firmware that was tested and failed, or had Beta firmware that was NOT tested because the firmware notes did not indicate a fix specifically for fragmentation.

- CSCdu87521

  The following message might appear when a connection using the EnterNet 300 version 1.4 PPPoE software and transferring via FTP:

  93 09:42:06.020 08/02/01 Sev=Warning/2 IPSEC/0xE3700002 Function CniInjectSend() failed with an error code of 0xe4510000 (IPSecDrvCB:517)

  This does not interfere with your connection. You can ignore this message.

- CSCdv40009

  When Zone Alarm's Internet setting is set to high and the VPN Concentrator sends a CPP firewall policy that allows inbound traffic on a specific port, the CPP rule takes precedence over the Zone Alarm rule allowing the specified port to be open.

- CSCdv42414

  Importing a PKCS12 (*.p12 or *.pfx) certificate using the Certificate Manager that has not been password protected will fail with the following error:

"Please make sure your import password and your certificate protection password (if for file based enrollment) are correct and try again."

Workaround:

Get a *.p12 certificate that has been password protected.

- CSCdv44529

  Attempting to install/uninstall Gemplus Workstation version 2.x or earlier while the Cisco VPN Client and its GINA (csgina.dll) is installed will cause the following error, and Gemplus will not install/uninstall:

  "A 3rd party GINA has been detected on your system. Please uninstall it before installing this product."

  Workaround:

  Do *one* of the following:

  – Uninstall the VPN Client and reinstall it after Gemplus software.

  or

  – Use Gemplus version 3.0.30 that no longer installs the gemgina.dll

- CSCdv46591

  When a CPP Firewall policy is in place that drops all inbound and outbound traffic and no WINS address is sent to the VPN Client from the 3000 series Concentrator, Start Before Logon fails. If a WINS address is in place, Start Before Logon works fine. Also, if a WINS address is sent and the CPP rule drops all inbound traffic, but allows all outbound traffic, Start Before Logon works fine.

- CSCdv46937

  Using the Aladdin "R2" model etoken, certain functions can be performed using the certificate even after the R2 token has been detached from the system (USB port). The VPN Client, for instance, can perform an IKE rekey without the token attached to the system. The reason for this is the design of the "R2" etoken: it does not contain the RSA key functions needed and must upload the private key to the system for these functions.

  In contrast, the Aladdin "PRO" etoken must be connected to the USB port during an IKE rekey, otherwise the VPN Client connection terminates. This is Aladdin's problem; it is not a VPN Client problem.

- CSCdv55730

  Using the Solaris VPN Client, some applications are unable to operate properly. A possible indicator of the problem is that a large ping is unable to pass through the VPN Tunnel.

  An MTU issue currently exists with the Solaris VPN Client that causes fragmentation errors that might affect applications passing traffic through the VPN Tunnel.

  To identify whether the VPN Client is properly fragmenting packets, use the following commands:

  ping -n <known good ping target address>

  ping -n -s <known good ping target address> 2500

  The first command ensures that the target is reachable, and the second determines whether fragmentation is an issue

  Workaround:

Step 1 1) Before opening the tunnel, bring down the MTU of the point-to-point interface to the MTU of the rest of the path to the concentrator (generally 1500). This would allow large packets to pass through, when using IPSec over UDP. No problems exist when using normal IPSec or cTcp.

Step 2 2)IP Compression may be set to “LZS” in the VPN Group on the Concentrator. This decreases the size of the encrypted packet and may allow the smaller packet to avoid fragmentation. If NAT is being used, switching the NAT method of the client from cTCP (TunnelingMode=1) to UDP (TunnelingMode=0) may also reduce the size of the packet.

- CSCdv62613

  When you have multiple VPN Client connections behind Linksys Cable/DSL router, the following problem can occur. Due to a Linksys problem with firmware versions 1.39 and 1.40.1, making multiple VPN Client connections enabling the feature “Allow IPSec over UDP” (transparent tunneling) may cause data transfer problems.

Allow IPSec over UDP is a VPN Client feature that allows ESP packets to be encapsulated in UDP packets so they traverse firewall and NAT/PAT devices. Some or all of the clients may not be able to send data. This is due to a Linksys port mapping problem, that Linksys has been notified of.

Workaround:

If possible, do not use the "Allow IPSec over UDP" (transparent tunneling) feature when you have multiple VPN Client connections behind Linksys Cable/DSL router.

- CSCdv67594

  The following Microsoft Outlook error might occur when the VPN Client connects or disconnects. This occurs when Microsoft Outlook is installed but not configured.

  ```
  Either there is no default mail client or the current mail
  client cannot fulfill the messaging request. Pun Microsoft
  Outlook and set it as the default mail client.
  ```

  To set Microsoft Outlook as the default mail client, right-click on the Outlook icon, go to Properties, and configure it to use Microsoft Exchange or Internet Mail.

- CSCdv73541

  The make module process fails during installation of the VPN Client for Linux.

  Workaround:

  The module build process must use the same configuration information as your running kernel. To work around this problem, do one of the following:

  – If you are running the kernels from Red Hat, you must install the corresponding kernel-sources rpm. On a Red Hat system with kernel-sources installed, there is a symlink from /lib/modules/2.4.2-2/build to the source directory. The VPN Client looks for this link first, and it should appear as the default value at the kernel source prompt.

  – If you are running your own kernel, you must use the build tree from the running kernel to build the VPN Client. Merely unpacking the source code for the version of the kernel you are running is insufficient.

- CSCdw60866

  Getting Entrust certificates using SCEP does not get the Root CA certificate. The Entrust CA does not send the whole certificate chain when enrolling with SCEP. Therefore, making a VPN Client connection might require the manual installation of the Root certificate before or after SCEP enrollment. Without the existence of the Root CA certificate, the VPN Client fails to validate the certificate and fails with the following VPN Client event/error messages:

  “Get certificate validity failed”
  “System Error: Unable to perform validation of certificate <certificate_name>.”

- CSCdw73886

  If an attempt to load the VPN Client is made before the Clients Service loads, the following error occurs: “The necessary VPN sub-system is not available. You will not be able to make a connection to the remote IPSec server.”

  Workaround:

  Wait until the Service has loaded, then start the VPN Client.

- CSCdx04343

  A customer had problems enrolling the Mac OS version of the VPN Client. Following some troublesome attempts at debugging the enrollment of the MacOS VPN Client with a Baltimore CA, it was felt that the Documentation should be improved and the Certificate Manager enhanced.

  Workaround:

  It seems that the critical thing as far as Baltimore is concerned is to put either or both of the challenge phrase (-chall) and the host's FQDN (-dn) in the request. This appears to be similar for the successful SCEP enrolment in a Verisign Onsite PKI. Perhaps there's a case for tweaking the interface a bit, or at least making some notes in the manual!

  Just doing cisco_cert_mgr -U -op enroll only asks for a Common Name, which is not enough. The request that succeeded on two separate Baltimore installations, one of which had an expired RA certificate, was as follows (switches only shown for brevity):

  cisco_cert_mgr -U -op enroll -cn -ou -o -c -caurl -cadn -chall -dn

The ou is required for connecting to a Cisco 3030 VPN Concentrator and is the group name. On almost every attempt, the certificate manager dies after starting to poll the CA, with an error in the log: “Could not get data portion of HTTP request”.

If this happens, it is possible to resume the enrollment with cisco_cert_mgr -E -op enroll_resume. The last attempt didn't fail at all though, and the certificate manager kept running until the request was approved, which is how it should behave.

- CSCdx57197

  If IOS sends a split tunnel attribute that is host-based (255.255.255.255 mask), the VPN Client uses the host in a QM, but it passes the IPV4_ADDR_SUBNET in the ID payload.

  IOS expects IPV4_ADDR, as this is a host ID. This causes connectivity issues.

- CSCdx51632

  If the computer is powered off or loses power during an MSI installation of the VPN Client, the VPN Client may not be registered in Control Panel, and the following may occur when attempting to reinstall:

  – A message may appear stating:
  Deterministic Network Enhancer Add Plugin Failed
  Click the “OK” button.

  – Error 1722. There is a problem with this Windows Installer package. A program as part of the setup did not finish as expected. Contact your Support personnel or package vendor. Click the “OK” button.

  – Error 1101. Error reading from file c:\config.msi\laff4.rbs. Verify that the file exits and you can access it. Click the “OK” button.

  – Error 1712. One or more of the files required to restore your computer to its previous state could not be found. Restoration is not possible. Click the “OK” button.

  After clearing the last message box, restart MSI installation. It should successfully install the VPN Client.

- CSCdx69189

  The Linux, Solaris, and Mac OS X platforms never seem to time out when left idle with the VPN Client connected, even after they've lost their connection to the concentrator.

The Dead Peer Detection (DPD) implemented on the VPN Client is triggered only if traffic is attempted through the tunnel. Once the client realizes it received no response to this traffic, it enters its worry loop for DPD. An idle platform that does not attempt to use the tunnel cannot detect the loss of a connection, even if the concentrator has been power cycled days before.

Checking the tunnel statistics does NOT alert the user to a lost connection.

Workaround:

Attempt to pass traffic through the tunnel. Once traffic has been generated, the VPN Client connection can determine within 5 - 12 minutes whether the connection is lost.

It might be easier to disconnect and reconnect a connection prior to use if it has remained idle for a prolonged period of time or if known connectivity issues are frequently seen with the user's connection.

- CSCdx70223

  The VPN Client's xauth dialog always stays in the foreground so it doesn't get "lost" (on XP it goes to the background and then jumps forward within seconds). The xauth dialog does not have focus, however, and it can be difficult to enter the username/password without first clicking on it with the mouse. This was observed on Windows 2000 and Windows XP; we have not checked Windows 98.

- CSCdx72463

  Installing the VPN Client using the Microsoft Windows Installer (MSI) displays "Time Remaining" for the installation. This time is not very accurate and should be ignored.

- CSCdx77292

  Microsoft article Q234859 states that for the resiliency feature to work on Windows 4.0, IE 4.01 sp1 and shell32.dll version 4.72.3110.0 or greater must be installed on the computer.

- CSCdx78868

  The Microsoft Installer (MSI) resiliency (self healing) feature does not restore all files that are installed with the VPN Client. The files that will be restored are files that are associated with the shortcuts under Start | Program Files | Cisco Systems VPN Client.

- CSCdx81491

  An issue can occur when using the Release 4.0VPN Client with Start Before Logon (SBL), after enabling SBL. The first time you log out of Windows, the VPN Client does not load after you press the CTRL+ALT+DEL key combination at the Windows logon prompt.

  Workaround

  Reboot the PC after enabling Start Before Logon; after a subsequent logout, the VPN Client should operate properly.

- CSCdx83687

  The following error occurs after the resiliency feature has reinstalled a missing file on Windows NT 4.0:

  > c:\winnt\profiles\all users\start menu\programs\cisco systems vpnclient\xxx.lnk
  >
  > The Windows installer failed to install the program associated with this file.
  >
  > Please contact your system administrator.

  xxx.lnk is whatever file is being restored.

  When you click OK, the PC reboots and the file *is* restored. The resiliency feature is working, but the error should not appear.

- CSCdx88063

  When attempting to launch the dialer when the dialer is already running on the logon desktop (due to SBL or SBL and AI), the following error occurs instead of the VPN Client dialer loading.

  "Single dialer instance event creation failed with error 5."

  This is most likely to happen when Start Before Logon and Auto Initiate are being used on a Windows NT/2000/XP system.

  Workaround

  This is due to the fact that the VPN Client dialer is already running on the "logon desktop". Most likely during Windows logon the dialer launched and posted an error, the Windows logon was completed and the error was never closed. To work around this error, do the following:

Step 1 Press CTRL+ALT+DEL to get to the logon desktop.

Step 2 Look for and close any VPN Client error dialogs.

Step 3 Press ESC to return to the normal Windows desktop; the VPN Client should load normally.

- CSCdy13425

  Connecting the Cisco VPN Client (versions 3.5 and later) to an IOS VPN device running 12.2(8)T using digital certificates might disconnect during a rekey. The connection could disconnect sooner if dead peer detection (DPD) is being used. The problem is under investigation.

  Workaround:

  Keeping the rekey times as high as possible will help avoid the problem.

  The other alternative is to use the VPN Client with preshared keys, which does not have the problem.

- CSCdy14218

  During installation of the VPN Client on a PC that already has the Enternet v.1.5c or v. 1.5c SP2, the following error might appear:

  "SVCHOST.EXE has generated errors and will be closed by Windows."

  Workaround:

  If this message appears, click OK, then reboot the PC when the VPN Client prompts for the reboot. After this, The message does not reappear and all connections work fine.

- CSCdy30098

  While using the Solaris VPN Client and its pppd 4.0 driver over PPPoE, the VPN Client can make a connection, but not pass any traffic.

  Due to an initialization issue in the VPN Client code, the Solaris VPN Client cannot pass traffic if it is first used with a PPPoE connection exclusively. It must first have attempted an hme connection (even a failed one) to properly ready itself for the PPPoE connection.

  Workaround:

  Remove the IP Address of the hme0 interface before attempting a connection using the ifconfig hme0 0.0.0.0 command.

As an alternative solution, after rebooting a Solaris workstation, attempt a VPN Client connection while the PPPoE link is down. The user may have to assign a bogus address to the hme interface if it does not already have some address. The VPN Client connection attempt need not be able to make a successful connection. Once the connection has timed out, restore the PPPoE connection, then the VPN Client connection should be able to pass traffic normally until the device is once again rebooted.

- CSCdy50648

  InstallShield's “Tuner” application produces warnings and errors when validating the Cisco MSI installation package.

- CSCdy65549

  If a you install the Cisco VPN client and you are not a local administrator, but you are a domain user that has been added to the local administrator group, the install completes successfully, but you may get the error “VPN subsystem unavailable” when trying to use the VPN Client, and you will be unable to use the VPN Client.

  If the user installing the VPN Client is a local administrator, then the error does not occur when running the VPN Client.

  Workaround:

  Log in as a local administrator when installing the VPN client.

- CSCdy68888

  On a Windows 98 PC that has the Sygate Personal Firewall, the following message may appear in the VPN Client log file:

  “Packet size greater than ip header”

  This message does not interfere with the VPN Client’s ability to pass data and can be ignored.

- CSCdy70168

  A user with the VPN Client cannot establish an IPSec tunnel to a VPN Concentrator running over an Internet satellite connection.

  There are three observed results:

  – User is never prompted for XAUTH username and password.

  – After successfully authenticating, the user cannot transmit/receive any data.

  - After successfully transmitting data for approximately 5 minutes, the VPN session is disconnected regardless of the user activity at the time of disconnect.

  This problem occurs only if IPSec over TCP is used.

  Workaround:

  Use IPSec over UDP.

- CSCdy76131

  If using the VPN Client feature Start Before Logon and the Sygate Personal Firewall version 5.0 build 1175 or later, the following Sygate configuration may be required in order to successfully log in to the domain after making a connection.

Step 1 Create Advanced rules to allow outgoing TCP ports 88, 445 and 1027.

Step 2 Turn off netBIOS protection in the Tools | Options menu on the Security tab.

Step 3 Disable Driver Level Protection in the Tools | Options menu on the Security tab.

Step 4 Allow the Cisco VPN Client to use the network in the Application dialog.

- CSCdy79358

  The following error might occur on Windows 98 when making many VPN connections without closing the VPN Client between connections:

  VPNGUI caused an invalid page fault in module MSVCRT.DLL at 0167:78002f52.

  To avoid this error, exit the VPN Client after disconnecting.

- CSCdz14583

  When installing the Release 4.0 VPN Client on Windows 2000, a driver signing warning appears, asking whether or not to continue the installation.

  The Release 4.0 VPN Client, when installed on Windows 2000 or Windows XP has a new Virtual Adapter feature. On Windows 2000 systems, the VPN Client installs a Virtual Adapter driver that is not yet signed, so when installing the VPN Client on Windows 2000 systems, a warning might appear.

  Workaround:

If during VPN Client installation a message pops up, click “Yes” to continue on Windows 2000.

- CSCdz48584

  The VPN Client on Windows XP using native XP PPPoE client fails to connect when using IPSec/TCP.

  Workaround:

  Make sure that the Windows XP Internet Connection Firewall is disabled for the PPPoE connection. This feature defaults to enabled when the connection entry is created. To disable it do the following.

Step 1 Run Control Panel, then click on Network Connections.

Step 2 Right click on the PPPoE connection entry (may be called “Broadband”) and select “Properties”.

Step 3 Change to the Advanced Tab and uncheck the “Internet Connection Firewall” option.

- CSCdz56076

  Some AOL applications may not be usable while a 4.0 VPN Client connection is active. These include the AOL integrated web browser and some internal links. Using external web browsers and other applications should work over the VPN. These issues were seen most recently using AOL version 7.0 and 8.0.

- CSCdz71367

  To connect to a VPN 3000 Concentrator requiring Sygate Personal Firewall, Sygate Personal Firewall Pro, using Are You There (AYT), the version of the firewall must be 5.0, build 1175 or later. The VPN Client might not detect an earlier version of the Sygate Personal Firewall and therefore, a connection will not be allowed.

- CSCdz74310

  After upgrading, the VPN Client is unable to connect to the VPN 3000 Concentrator. The ability for the VPN Client to negotiate an AES-192 IKE Proposal has been removed. This change affects all VPN Client versions greater than 3.7.2.

Workaround

Reconfigure the VPN Concentrator so that it does not require an AES-192 IKE Proposal for VPN Client connections.

- CSCdz75892

  The Equant remote access dialer does not automatically connect the Release 4.0 VPN Client, as it could when using the Release 3.x VPN Client. If you have the Equant dialer configured to establish your VPN connection, the VPN Client appears, but you must manually click Connect to connect.

- CSCdz76316

  Disable the VPN Client log, stops logging to the file and screen. Re-enabling logging first clears the screen and reloads all the text from the file back to the screen. Log output should start to appear on the screen and file.

- CSCdz76770

  With the version 4.0 Cisco VPN Client installed, you are unable to browse the web, and when you try, you are redirected to the following URL: http://lockup.zonelabs.com/8083.html. The web browser displays a message like “Notice from Zone Labs Internet Security” and directions about reinstalling Zone Alarm personal firewall.

  Workaround:

  Cisco VPN client version 4.0 includes firewall functionality from Zone Labs Inc. It is possible that a failed Zone Labs uninstall left an incorrect value in the systems registry and must be changed. To resolve the problem follow these steps.

Caution This procedure contains information about editing the registry. Before you edit the registry, make sure you understand how to restore it if a problem occurs.

Step 1 Restart the computer and when your computer screen displays the startup message like “Starting Windows...” and a progress bar at the bottom of the screen, press the F8 key on the keyboard. This should display an advanced options screen.

Step 2 At the advanced options screen select “Safe Mode” as a startup method.

Step 3 If prompted, login to the PC once it is booted (you must have Administrator rights to login in Safe Mode).

Step 4 Click Start > Run and type “regedit” in the Open: box (without the quotes) and click OK. This launches the Windows registry editor.

Step 5 In the registry editor, browse to the following path: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\vsdatant and select the Start parameter in the right pane.

Step 6 Right-click Start and select Modify. In the Value data: field enter the number 3.

Step 7 Click OK and exit the registry editor.

Step 8 Restart the computer and boot normally; the problem should be resolved.

- CSCdz87404

  The 4.0 VPN Client (on Windows 2000 or Windows XP) connects but is unable to pass data over the VPN tunnel. Viewing the routing table using “route print” at a command prompt shows the default gateway has been modified incorrectly as in the example below.

  0.0.0.0 255.255.255.255 n.n.n.n n.n.n.n 1

  Where n.n.n.n is the IP address assigned to the VPN.

  Workaround:

  This is due to a misconfiguration on the VPN3000 at the central site. Make sure that the Group | Client Config settings for Split Tunneling Policy are correct. If the group is set to “Only tunnel networks in the list” and the Split Tunneling Network List is the predefined “VPN CLient Local LAN” list this problem will occur.

  If split tunneling is the desired result, change the Split Tunneling Network List to an appropriate list, otherwise make sure that the Split Tunneling Policy is set to “Tunnel Everything” and check “Allow the networks in the list to bypass the tunnel”. This allows for proper Local LAN functionality.

- CSCdz87487

  The following configuration will allow inbound ICMP packets (pings) when the default firewall rule for the Centralized Protection Policy (CPP) is pushed to the VPN Client.

  On the VPN Client:

  – Stateful Firewall (Always On) is enabled.

- The setting “StatefulFirewallAllowICMP=1” is added to the [Main] section of the vpnclient.ini file.
- A connection is made to the VPN Concentrator that pushes the default CPP firewall rule to the VPN Client.

The parameter, “StatefulFirewallAllowICMP=1” should only be used if it is desired that ICMP traffic be allowed to pass through the firewall.

- CSCea03597

  When the VPN Client is installed and Start before Logon is configured, logging into an Active Directory Domain might take a long time, with or without a VPN connection.

  This issue occurs under the following conditions:

  - The VPN Client is installed on Windows 2000 or Windows XP Professional.
  - You have enabled “Start before Logon” in the VPN Client.
  - You are logging in to a Windows Active Directory domain (not an NT 4 Domain).

  Workaround:

  This problem occurs because of a fix that was added for CSCdu20804. This fix adds the following parameter to the registry every time Start before Logon is enabled:

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetLogon\Parameters

  ExpectedDialupDelay

  Removing “ExpectedDialupDelay” from the registry (then rebooting) should fix the problem with slow logons to an Active Directory Domain.

Caution This procedure contains information about editing the registry. Before you edit the registry, make sure you understand how to restore it if a problem occurs.

Note If you disable, then re-enable Start before Logon, this entry is added again and must be removed.

- CSCea16012

  The Firewall Enhancement, “Prevent VPN Traffic Blocking”, automatically adds the Loopback address (127.0.0.1) and the address of the VPN 3000 Concentrator to the ZoneAlarm or ZoneAlarmPro trusted zone.

  An exception to this, however, occurs if the VPN Client is installed before Zone Alarm. Then the VPN Client’s service must be restarted by rebooting the PC or stopping and restarting the service through Control Panel (on Windows NT-based PCs).

- CSCea16482

  If the Digital Certificate you are using has expired, the Windows VPN Client GUI does not popup with an error message indicating it has expired. The only indication you have is in the log file.

  A message does appear if you are using the VPN Client command line - vpnclient.exe

- CSCea17705

  If a ZoneLabs product such as ZoneAlarm or ZoneAlarm Pro is installed on the PC and the VPN Client is installed or upgraded, ZoneAlarm blocks the VPN Client service (cvpnd.exe). The VPN Client’s splash screen appears, but the GUI does not. ZoneAlarm does not ask the user whether to allow the VPN Client to access the Internet. Additionally, the following error appears after about two minutes:

  “The necessary VPN sub-system is not available. You can not connect to the remote VPN server.”

  Workaround:

  Do the following steps:

Step 1 Open the ZoneLabs product and select “Program Control”.

Step 2 Click on the “Programs” Tab

Step 3 Cisco Systems VPN Client's Access permission is a ?. Click under “Trusted” and select “Allow”. The ? mark changes change to a Check mark.

Step 4 Reboot the PC.

Step 5 When the PC boots back up, the client will launch normally.

- CSCea25682

  The following Notification might occur if the Cisco Systems Integrated Client is required to make a connection.

  "The Client did not match the firewall configured on the central site VPN device. Cisco Systems Integrated Client should be enabled or installed on your computer."

  When this occurs, the connection is not allowed. If this Notification appears, click Close and attempt to reconnect. If this second attempt to connect fails, reboot the PC. The connection should succeed at this point.

- CSCea25991

  Upgrading ZoneAlarm Pro version 3.5.xxx to ZoneAlarm Pro version 3.7.098 when the VPN Client is installed on the PC might cause the following error to appear:

  > "The procedure entry point DbgProcessReset could not be located in the dynamic link library VSUTIL.dll."

  Click OK, and the installation continues.

- CSCea27524

  This problem has two facets. You cannot select text from the VPN Client log tab, and trying to save the VPN Client log results in an empty (zero byte) file. This problem might occur if the VPN Client logging has been enabled, disabled, or cleared.

  Workaround:

  If the all or part of the log must saved, you can select the text with the mouse or by using CTRL+A, and then copy it using CTRL+C. You can then paste it as usual using CTRL+V in Notepad or your favorite editor.

  As an alternative, the VPN Client log files are saved to the directory c:\Program Files\Cisco Systems\VPN Client\Logs by default and can be opened and viewed using a text editor and saved as a different name if needed.

- CSCea29976

  After the user enters the username and password, the VPN Client machine may go blank for a moment and then continue. This behavior has not shown any negative effect on the tunnel connection or the user's ability to use the PC.

- CSCea30026

  The 4.0 VPN Client running on Windows 2000 or Windows XP is unable to connect. The following event appears in the log.

  "The Client was unable to enable the Virtual Adapter because it could not open the device."

  This can happen as a result of the VPN clients virtual adapter not being installed.

  Workaround:

  Sometimes the "Driver Signing" setting in Windows can cause the virtual adapter to not be added during VPN Client installation. To check your Driver Signing setting, perform the following steps. If it is set to "Block", change it to "Warn" and reinstall the VPN Client.

Step 1 Launch Control Panel

- Windows 2000:

  Start->Settings->Control Panel

- Windows XP:

  Start->Control Panel

Step 2 Double click on the System applet, switch to the Hardware tab and then click the "Driver Signing" button.

- CSCea31192

  When the Checkpoint VPN-1 Securemote client is installed with the 4.0 VPN Client, and the VPN Client attempts to connect using cTCP, the 4.0 VPN Client cannot make the connection. Connections work with UDP, NAT-T, and non-NAT connections.

  Workaround:

  To make a connection with cTCP when the Checkpoint VPN-1 Securemote is installed, you must disable the Check Point SecuRemote driver in the Connections Properties. To do this, you must be administrator. Follow these steps:

Step 1 Click Start > Settings > Control Panel >Network and Dial-up Connections.

Step 2 Select the Local Area Connection you use.

Step 3 Click on File > Properties.

Step 4 Uncheck Check Point SecuRemote, and click OK.

- CSCea34282

  Using dialup entries with Japanese Characters does not work.

- CSCea43117

  The following error message might occur during VPN Client installation:

  IKernel.exe - Application Error

  The instruction at “0x771c741a” referenced memory at “0x00163648”. The memory could not be “read”.

  This error is caused by an InstallShield component, possibly because of a run-once stale remnant.

  Workaround:

  Reboot.

- CSCea44601

  The VPN Client does not put any limit to the number of log files that are saved in the \VPN Client\Logs directory. Users must manually delete these files to remove all or some of them.

- CSCea52757

  When installing from a CD, where all the files are Read-Only by default, the MSI installer copies the VPNCLIENT.INI and .PCF files to the destination but does *not* change the file attributes from Read-Only to Read+Write.

  Workaround:

  Manually change these files Read+Write after the installation.

- CSCea62229

  Using the 4.0 VPN Client with Entrust Entelligence certificates, the “Send CA Certificate Chain” option should be grayed out and unavailable, but it is not.

Workaround:

Checking the “Send CA Certificate Chain” option when using Entrust Entelligence certificates makes the VPN Client connection fail to complete, leave this option unchecked.

- CSCea63957

  If you uninstall the VPN Client from a Windows 2000 or Windows XP Computer with RASPPPOE, the following message box might appear:

  > Failed to uninstall the Cisco Network Adaptor.
  > Error: 0xe000020b

  Click OK. The Client uninstallation then continues normally.

- CSCea65393

  Using the 4.0 VPN Client with the virtual adapter (Windows 2000 or Windows XP) in a multiple NIC environment, the VPN Client might not pass data while connected.

  When the VPN Client PC has multiple network interfaces and the default gateway is on the non-VPN interface, the default gateway metric is not incremented. This might result in data that is bound for the VPN going to the non-VPN default gateway and being dropped. This problem is clearly identifiable by looking at the routing table while a VPN (All Tunneling) connection is active, where the two default routes appear with equal metrics.

  Workaround:

  Manually increment the local interface metric by 1. Then the VPN Client’s virtual adapter has a lesser metric and is the best route.

- CSCea66549

  If two or more VPN Clients (running on Windows 2000 or XP) are connected to a VPN 3000 Series Concentrator and receive firewall policy from a ZoneLabs Integrity Server, the Integrity Server only registers one connection.

  On the Integrity Flex (client agent), under “Policies”, the “Integrity Server” column flashes “Connected” then “Disconnected” over and over. Also, the VPN Client log includes the following event: “The firewall, configured for Client/Server, returned a status of lost connection to server.”

  Workaround:

  Cisco is actively working with Zone Labs to provide a patch to their Integrity Server software to address this issue. There is no workaround at this time.

Customers using Integrity should not upgrade to version 4.0 of the VPN Client at this time.

- CSCeb37161

  Using the Mac OS X VPN Client, Release 4.0 or higher, a profile using certificates works fine with the Command Line Interface client, but fails to connect with the VPN Client GUI. The Release 4.0 VPN Client fails to connect, while the Release 4.0.1.A VPN Client warns that the certificate cannot be found. The VPN Client GUI requires the "CertSubjectName" field to be filled out in the profile when using certificates. The CLI does not fill in this line or require it.

  Workaround:

  Using the GUI, modify the profile and select the proper certificate and same the profile. This fills in the GUI required "CertSubjectName" field. Initially, creating the certificate profile in the GUI also bypasses this issue.

- CSCec43986

  After upgrading to 4.0.1D or E concentrator tries to authenticate users to the Base Group

  Errors seen on the logs add extra characters to the GROUP

  Workaround:

  Use 4.0.1C or earlier version.

Caveats Resolved in Release 4.0.3

Release 4.0.3 resolves the following issues:

- CSCec01510

  Windows VPN Client (version 4.x) fails to connect to a VPN 3000 Series Concentrator from a Windows Terminal Services Connection. This was possible with earlier 3.6.x versions. The problem occurs when a user connects to a Windows 2000 server running terminal services and from the terminal services session launches the VPN Client to connect to a VPN 3000 Concentrator (configured to do split tunneling). With versions4.x using the new Virtual Adapter, this is not possible; however, it was possible with versions 3.6.x.

- CSCdz25788

  When using the VPN Client, Release 3.6.2B on Windows XP PCs, if “register this address to DNS” was not Checked on a PPP adapter side, Split-DNS behavior differs.

  – If checked, Split-DNS behaves normally.

  – If not checked, Split-DNS functions normally, but after disconnecting from the internet, it never refers to the DNS of the Internet side.

- CSCeb47765

  Name resolution can take up to 40 seconds when a tunnel has been established. This problem occurs only on WIN XP. This problem was not evident in 3.6.x VPN Client code.

- CSCeb67454

  Symptom: With the VPN client 4.x on XP split tunneling and split DNS, the DNS lookup does not use DNS servers.

  The following observations pertain to this issue:

  – All or nothing tunnel works fine.

  – This problem is only seen with split tunnel & split tunnel with split DNS

  – If you use nslookup to resolve the PINGed server, it might give the right info.

  – This problem exists for both FQDN and unqualified name.

Caveats Resolved in Release 4.0.2.E

Release 4.0.2.E resolves the following issue:

- CSCeb80558

  If vpnclient.ini option “AppendOriginalSuffix” has a value of 1 or 2, the VPN Client should append the primary suffix of the machine at tunnel establishment.

Caveats Resolved in Release 4.0.2.D

Release 4.0.2.D resolves the following issues:

- CSCdy67438

  VPN Client, Release 3.6.2 is installed on the Windows 2000 and Windows XP machines using the customized (OEM) installation (InstallShield Install).

  To activate “Start before Logon”, oem.ini and vpnclient.ini are present in the installation package. Once the machine is rebooted after the installation, the “Start before Logon” feature does not work.

- CSCeb12483

  When making changes to the vpnclient.ini and preceding [CertEnrollment] parameters with an exclamation point (!) character, the fields are still editable after installation. The exclamation point should make these fields uneditable, but users can still edit the fields after installation and rebooting.

- CSCeb27643

  Information like Department information does not get filled in using v4.0.1 of the VPN Client. When using Certificate Enrollment, the CA url info is correctly saved, but other information is ignored.

- CSCeb66861

  On an XP PC with the 4.0 or 4.0.1 VPN Client, a user may experience DNS issues upon connection. After connecting to a VPN 3000 Concentrator (Release 4.0), the VPN Client can ping resources on the private network by IP, but not by name. Once this happens on the XP PC, you can go to network connections->advanced->advanced settings and change the order of the adapters, or actually move a different (doesn't matter which) one to the top of the list and hit OK. You can then ping by name.

  If you disconnect the VPN Client and reconnect, you get the same results, but the adapter at the top of the list is the one you moved there previously. You cannot ping by name until you move a different adapter to the top of the list and hit OK.

- CSCeb70819

  The VPN Client intermittently takes as much as 30 seconds to launch. This happens only intermittently. It takes about 15 seconds for the splash screen to come up, and another 15 seconds for the GUI to come up. If you launch the GUI from the command line or Windows Explorer by executing vpngui.exe directly, it takes half that time.

  This problem exists only in Releases 4.0.2, 4.0.2.A and 4.0.2.B of the VPN Client. If VPN Client logs are disabled, this problem completely goes away.

- CSCeb74792

  The silent uninstall feature of the VPN client does not uninstall the Profiles and certificates folder from the Program Files folder.

  C:\Program Files\Cisco Systems\VPN Client

- CSCeb80558

  If vpnclient.ini option “AppendOriginalSuffix” has a value of 1 or 2, the VPN Client should append the primary suffix of the machine at tunnel establishment.

Caveats Resolved in Release 4.0.2.C

Release 4.0.2.C resolves the following issues:

- CSCdz57585

  There is no way to prevent the “sample.pcf” file from appearing in the VPN Client connection entries after installing the Mac VPN Client GUI. It is unnecessary to see “sample.pcf” in the GUI connection entries. It should remain as a template for hand-made profiles but not appear on the GUI. The Windows VPN Client already behaves in this fashion.

- CSCea35578

  After waking from a workstation sleep, the Mac VPN Client still shows that it is connected, even though it is not tunneling or blocking any traffic.

  If the VPN Client is connected when the workstation is put to sleep, it might not realize that it has lost its connection.

- CSCeb21138

  At VPN Client initialization, the version string is overlaid in text on top of the splash screen. There is no may to modify this string for OEM customization. It should be removed.

Caveats Resolved in Release 4.0.2.B

Release 4.0.2.B resolves the following issues:

- CSCeb04745

  Can't install Cisco System Virtual Adapter after removing a VPN 5000 Client. This occurs because some of the VPN 5000 Registry keys are not removed by the Uninstall procedure.

- CSCeb19862

  VPN Clients, version 4.0.x, do not produce an informative Delete with Reason message when the VPN Concentrator has been configured to disconnect the Client due to "Type and Version Limiting".

  Type and Version Limiting was introduced with the 4.1 Concentrator code and does not trigger an informative message from the VPN Client. The current message is:

  Secure VPN Connection terminated by Peer.

  Reason: Unknown Error Occurred at Peer.

- CSCeb40034

  The VPN Client is terminating the connection prematurely during rekey.

  The scenario is:

  1. The initial IKE SA (SA1) comes up.
  2. Rekey is initiated. P1 is complete by establishing SA2.
  3. Xauth is in progress.
  4. SA1 is deleted. In this case, the remote peer sends a Delete message.
  5. The VPN Client detects that there is no user authenticated IKE SA in the system and brings down the connection.

Although SA2 is not yet authenticated, it is still a valid IKE SA. The VPN Client should not bring down the connection at this point and should let the rekey complete.

- CSCeb52019

  DNS suffix search list gets replaced when CVPN Client 4.x is used for VPN tunnel establishment.

- CSCeb54855

  Unable to autopopulate the CertSerialHash value in the .PCF file. The customer creates a customized profile and installs the certificate in the Personal store on the PC. When the end user uses the VPN Client for first time, it does not populate the CERTSERIALHASH value under the .PCF file, which was working in earlier code.

Caveats Resolved in Release 4.0.2.A

Release 4.0.2.A resolves the following issues:

- CSCeb35709

  The VPN Client does not handle stdin / stdout data correctly.

- CSCeb38492

  The VPN Client user interface terminates unexpectedly with the following error when a third-party dialer is misconfigured or the Client can't find the dialer at the path specified.

  > vpngui.exe has generated errors and will be closed by Windows. You will need to restart the application. An error log is being created.

  If you specify the path correctly, the error does not occur.

- CSCeb39137

  The TunnelEstablished flag is set to 1 (Connected) before user has accepted the banner. This is an issue now that Release 4.0 prevents communication across the tunnel before the banner is acknowledged.

Caveats Resolved in Release 4.0.2

Release 4.0.2 resolves the following issues:

- CSCdz32866

  The Macintosh OS X version of VPN Client does not save the location & size of the external Log Window so it must be resized and moved every time you open it.

- CSCdz58821

  Using the Linux version of the VPN Client over a SuSe native PPPoE connection, the VPN Client fails to connect. The Mandrake platform exhibits the same symptoms. The VPN Client is unable to bind to the type of PPPoE used natively by SuSe and Mandrake.

- CSCdz78215

  While attempting to make a connection using the Linux version of the VPN Client, the workstation crashes if PPPoE is activated during the connection. That is, if a VPN Client connection is in progress while PPPoE is being brought up, the workstation crashes.

- CSCdz88631

  When installing the Linux version of the VPN Client on a Red Hat 8.1 beta installation, a number of disquieting warnings appear during installation as well as a strange binary message while connecting the VPN Client. These messages do not affect the performance of the VPN Client.

- CSCea22263

  If the certificate which is to be used by the VPN client, contains the non-ASCII characters in the CN and Subject (letters with umlaut, various kinds of accents, copyright character), then after selecting the certificate in the VPN dialer, closing the VPN dialer, and reopening the same connection entry, there is an error message, “The certificate <name>, associated with this Connection Entry, no longer exists. Please select another certificate.”

  In the certificate list, though, this certificate is still present and can be selected.

- CSCea65315

Rebranding the VPN Client Release 4.0 for Mac OS X is not currently possible. If you drop a png file into the Resources folder of the installer disk image, when you install the VPN Client, the png file is not copied into the /etc/CiscoSystemsVPNClient/Resources/ folder.

- CSCeb00549

  The Linux VPN Client does not install on platforms with kernel versions of 2.5 or 2.6. These kernel versions are not yet supported with the 4.0 Release or any previous versions of the VPN Client.

- CSCeb07131

  Using the Windows 4.0 VPN Client with certificates, we are unable to disable certificate expiry message.

- CSCeb08604

  The VPN Client should treat profile names as case insensitive.

  If there is a profile *PROFILE1.pcf* and the following command is executed from command prompt:

  ipsecdialer /c /user <UserName> /pwd <UserPassword> profile1

  or

  vpngui /c /user <UserName> /pwd <UserPassword> profile1

  The above commands should work. "profile1" should NOT be treated as CASE SENSITIVE. This is a regression from 3.6 gui.

- CSCeb09593

  When the silent disconnect option is used with the VPN Client, the “You've been disconnected” dialog is still shown after a "VPNCLIENT DISCONNECT" is issued.

- CSCeb17553

  In the 4.0 version of the VPN Client, vpnclient.exe no longer supports the “-sd” command line option. If I have an old shortcut for vpnclient.exe that uses this option, I get a Usage output stating that this option is no longer supported. This breaks all the 3.x shortcuts that use this option.

- CSCeb35613

  Cvpnd.exe (Cisco VPN Service) crashes when trying to establish a tunnel. If you run into this problem, the last entry in the logs should say:

Unable to forward xAuth request data to xAuth application. Error code <error code>

This generally occurs if a severe error is encountered while trying to XAuth. Specifically, this happens if we can't spawn a process to do XAuth. Some reasons for that would be if some of the VPN Client execuatbles files are deleted or modified.

- CSCeb37036

  On rare occasions, the Release 4.0 VPN Client disconnects the tunnel right after establishing it. This happens only when using a dialup connection to Internet (or PPPoE).

  The following messages appear in the VPN Client logs:

  05 14:04:02.745 06/11/03 Sev=Warning/3 CM/0xA310002C

  Adapter address changed from <IP Address>. Current address(es): <Current IP Addresses>.

Caveats Resolved in Release 4.0.1

Release 4.0.1 fixes the following issues that existed in earlier software releases:

- CSCea39719

  When the vpnclient.ini has the setting, “StatefulFirewallAllowICMP=1”, and StatefulFirewall (Always On) is suspended, then resumed, the Stateful Firewall does not allow ICMP traffic to pass unless the service is stopped and restarted.

- CSCea47454

  Buttons in Certificates->Import/Export windows are truncated when using system Large Fonts (120dpi) setting.

- CSCea76011

  IPSec over TCP and/or Split tunneling does not work on certain machines. This issue is the same as CSCdz51629, and CSCdy80016. For example, using a Sierra SMC2632W wireless card, and building a VPN tunnel to a PIX firewall, if split-tunneling is used, then no SAs are built for the networks in the split tunnel list, resulting in no traffic flow over the tunnel.

- CSCea86293

When using the following command line:

ipsecdialer.exe /c /user USERNAME /pwd PASSWORD PROFILE

the VPN Client continually prompts for the password.

- CSCea88456

  When installing Release 4.0 of the VPN Client on Japanese Windows 2000, the virtual adapter installer hangs.

- CSCea93394

  This problem occurs only on the Windows version of the Release 4.0 VPN Client, not on non-Windows platforms or earlier versions of the VPN Client.

  When a tunnel is established, the central site Concentrator could send a DNS domain to be used by the VPN Client by mode configuration. The VPN Client makes the changes to the system to use the DNS suffix pushed by the central-site Concentrator. This works fine, but when the tunnel is disconnected, the DNS suffix change that was made when the tunnel connected is not undone.

- CSCeb00459

  When the Cisco VPN Client disconnects, it logs the following message in a file called faultlog.txt, located in C:\Program Files\Cisco Systems\VPN 3000 Client:

  27 22:50:50.401 04/27/03 Sev=Critical/1 CVPND/0xE3400001
  Microsoft IPSec Policy Agent service started successfully

  The message appears only when we disconnect the Client. The Client functions without any problems.

  The level for this message should be changed and this file should probably be documented.

Caveats Resolved in Release 4.0

This section lists the caveats fixed since Release 3.6.3 (Windows) or Release 3.7.2 (Linux, Solaris, and Mac OS X). If you have an account on CCO you can check the status of any caveat by using Bug Navigator II.

To reach Bug Navigator II on CCO, choose Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

- CSCdt42661

  When using the VPN Client behind an ESP-aware NAT/Firewall, the port on the NAT/Firewall device may be closed due to the VPN Client's keepalive implementation, called DPD (Dead Peer Detection). When a Client is idle, it does not send a keepalive until it sends data and gets no response.

  Refer to "Connection Profile Configuration Parameters" in the *VPN Client Administrator Guide* for a detailed description of creating profiles.

- CSCdv64330

  The VPN client cannot connect using digital certificates issued from an RSA Keon CA if the "Send CA certificate chain" option is selected. The feature defaults to disabled.

- CSCdw61796

  The Cisco VPN Client fails to connect while configured for digital certificates and posts the following error in the Log Viewer.

  "Get certificate validity failed"

  Some of the reasons this event could have occurred are:

  – The received certificate has an incomplete chain.

  – The received certificate is either expired or not valid yet. Check the time on the certificate.

- CSCdx89940

  A Restricted, Standard, or Limited user (Windows 2000) cannot install the VPN Client using the Windows Installer (MSI), even if elevated privileges are set for the user and the PC.

- CSCdy62397

  The following Blue Screen failure might occur on a Windows NT-based PC that has the Sygate Personal Firewall installed and has had a VPN connection going for three or more days:

  Stop:000000d1 (e572685c, 00000002, 00000000, bff110bc)

  ***Address bff110bc base at bff0f000, datestamp 3e1cdf98 -- Teefer.sys

- CSCdz07114

  For the Cisco VPN Client version 3.6 and earlier, you had the ability to replace Company Name, Product Name, bitmaps, icons, and the folder in which the Client was installed. For the new version 4.0 VPN Client this capability has changed somewhat.

- CSCdz09585

  If you select “Delete” from within the Certificate tab, you are prompted with the following message: “Are you sure you want to delete the certificate?” In that window, there is an 'X' in the upper right corner. Clicking the 'X' to close out the window instead of pressing one of the buttons, *deletes* the digital certificate.

- CSCdz24962

  In the Release 3.7 VPN Client GUI, the Certificate enrollment dialog where the user enters the DN information should include the DN field abbreviations after the field names in parenthesis; for example, “Common Name (CN):” or “Department (OU):” since much of the product documentation makes reference to “OU” for group selection.

  The common DN parameters are:

  – Common Name - CN

  – Email - E

  – Department - OU

  – Company - O

  – State - ST

  – Country - C

- CSCdz25064

  In the Release 3.7 VPN Client MacOS X GUI, the Certificates tab has a "Validity" tab. For a digital certificate that is not valid yet, it shows "invalid: expired on Jun 4, 2003 14:15:49" where it should display something like "not valid until <date> <time>" or at a minimum just state "expired or not valid yet" without the date and time to not be misleading.

- CSCdz25200

  The Release 4.0 VPN Client cannot currently import a Microsoft CAPI based certificate directly into the Cisco certificate store. The certificate must be manually exported from Microsoft Internet Explorer and then imported into the Cisco certificate store.

- CSCdz26241

  The Release 4.0 VPN Client prompts you to insert your Smartcard when loading even though you are not using certificates with the VPN Client.

  In this case, the VPN Client is installed on a PC with Smartcard-based certificates or Entrust Entelligence-based certificates. The VPN Client attempts to enumerate the list of installed certificates, including ones that are Smartcard- or Entelligence-based and may prompt the user.

- CSCdz26449

  On the Release 3.7 VPN Client Mac GUI, on a new installation of the VPN Client, the "Edit Settings" button launches the "Logging Options" window. When you do this, all logging levels are set to 3 by default. However, the vpnclient.ini logging levels are set to one. The default button is "Cancel". If a customer presses the Enter key, the levels stay at 1.

  The Logging Options window does not read from the vpnclient.ini file.

- CSCdz29463

  Using the Release 3.7 VPN Client, there is a parameter in the pcf files that controls whether the VPN Client allows the use of split DNS when connected. This value should default to 1, which means enabled. It currently defaults to 0, which makes the feature appear broken. Setting it to 1 in the pcf allows split DNS to function.

- CSCdz38680

  This issue applies only to the Release 4.0 VPN Client and only with Virtual Adapter (Windows 2000 and Windows XP). The VPN Client's local network happens to be of the same IP subnet as the remote private network. When a VPN connection is up data meant for the private network stays local; for example, 192.168.1.0/255.255.255.0

- CSCdz40609

  In a Windows 2000 or Windows XP environment, if the public network matches the private network (for example, a public IP address of 192.168.1.5, with a subnet mask of 255.255.0.0, and an identical private IP address) and the public network's route metric is 1, then traffic might not be tunneled to the private network. The same problem can occur if you are using a virtual adapter and the public metric is smaller than the virtual adapter metric.

- CSCdz48154

  If the parameter "StatefulFirewallAllowTunnelTraffic=0" is placed into the the [main] section of the vpnclient.ini and Stateful Firewall (Always On) is enabled, no inbound or outbound tunneled traffic will pass. Either remove this setting from the vpnclient.ini or set it to "=1".

- CSCdz52058

  If you attempt to Import a Connection Entry with the same name as one that already exists, you are asked if you would like to overwrite the existing entry. If you choose to overwrite the entry, an error appears and the `entry` is not overwritten.

- CSCdz56021

  For Release 4.0, Beta release 1, the Cisco VPN Client does not coexist with the Nortel VPN client. When version 4.0 Cisco VPN Client is installed on a system running an existing third party VPN client (for example, the Nortel client - not Microsoft), a conflict occurs with the services started by Cisco. This prevents other clients from successfully establishing remote access sessions.

- CSCdz74850

  The Release 4.0 VPN Client Statistics | Routes dialog displays a 0.0.0.0/0.0.0.0 entry even during a split tunnel connection.

This occurs only if the VPN Client has made an all-or-nothing connection prior to the split tunnel connection without exiting the VPN Client application between connections.

- CSCdz76582

  If you try to delete a personal Certificate, you are prompted only for the Certificate password, then the certificate is deleted. You are not given a second chance message like other certificates (root, subordinate, etc) where it says “Are you sure you want to delete the certificate?”

- CSCdz81671

  The Release 4.0 VPN Client, when using the virtual adapter (Windows 2000/Windows XP only) and Split DNS feature, might send all DNS requests over the VPN tunnel.

  Due to the addition of the virtual adapter in the Release 4.0 VPN Client, Split DNS functionality now partially depends on the Windows operating systems to choose the correct pass for DNS requests. DNS requests meant only for the VPN are sent only through the VPN. DNS requests that do not match the VPN domain suffixes will also go through the VPN when they should not.

- CSCdz83065

  Uninstalling the VPN Client using the Microsoft Installer (MSI) does not detect that the VPN Client is connected and the uninstall completes. We highly recommend you disconnect and exit the VPN Client before uninstalling.

  This issue occurs only if VPNGUI.EXE is hidden; that is, it is configured under Options | Preferences to “Hide upon connect” and you have the Client connected, or have just disconnected and it is still in the systray. Any time the GUI is open (unhidden) and an MSI uninstall is started, the presence of the VPN Client prevents you from uninstalling.

- CSCdz83461

  Unable to pass data after disconnecting the Release 4.0 VPN Client on Windows 2000 or Windows XP. The Release 4.0 VPN Client has a virtual adapter that could have failed to disable after disconnecting.

- CSCdz88476

  When Start Before Logon is configured on the VPN Client on Windows XP, and you install the Release 4.0 VPN Client, upon reboot you will see the following message for 1-2 minutes:

"System initialization in progress. Creating a secure connection to your network requires that MS networking be allowed to complete its initialization. If you do not wish to create a VPN connection to a remote network, you may click the CANCEL button..."

On subsequent reboots you will see this message, but it stays on the screen for only 5-10 seconds instead of minutes.

This problem also occur on Windows 2000, but a little differently. After installing and rebooting, and before you see the dialog that prompts you to press CTRL-ALT-DEL, you see a window that says "Preparing network connections...". During this time, there is a 1-2 minute delay which goes away after subsequent reboots.

- CSCdz88896

  The Release 4.0 VPN Client on Windows 2000 or Windows XP can connect but cannot pass data. This problem occurs only with the Windows 2000 or Windows XP when the VPN Client is connecting from an IP subnet that matches or closely resembles the private network that it is making the VPN connection to.

  This is most commonly seen in an environment where the VPN Client is behind a NAT device that is using a common private IP address range like 10.x.x.x.

- CSCea03326

  The feature that was added in Release 3.6.2 called "Automatic logoff after VPN" does not currently work in v4.0.

  This feature replaced Start before Logon for some users. It allows a user to establish a VPN connection first, and then the user is automatically logged out and the VPN connection is maintained. This allows the user to log into the Domain during the VPN connection, without the need for a custom GINA to be installed.

- CSCea04522

  When installing The VPN Client for Mac, version 4.0.int_73 over top of an earlier version of the VPN Client, it fails to unload the old NKE and load the new one.

  If you are upgrading from an earlier 4.0 version, "kextstat|grep cisco" returns nothing and returns you to a prompt. If you are upgrading from a 3.7.x VPN Client, "kextstat | grep cisco" returns both the old NKE and the new one.

If you reboot, the NKE loads correctly.

If you are upgrading from a previous 4.0 VPN Client, re-running the installer loads the NKE correctly.

Uninstalling the earlier version *before* installing the new version also works correctly.

- CSCea04814

  When using a Digital Certificate for VPN Client connections, there is no indication that your Certificate is about to expire. In previous versions of the VPN Client, 30 days before the certificate was set to expire, a message would pop up upon connection stating that your Certificate would expire soon.

- CSCea05185

  The InstallShield version of the 4.0 VPN Client, as well as 3.6 versions, do NOT detect an existing Cisco IT 3.5(A) VPN Client is installed on your PC and will install the new version right on top of old one. The VPN Client REQUIRES the old version to be uninstalled first or else the new installation may not properly update required files.

  If you are a Cisco employee, you MUST first check to see if you have the Cisco IT 3.5(A) version of the VPN Client installed and manually uninstall it before installing the 4.0 VPN Client.

- CSCea05304

  The 4.0 VPN Client feature, Delete-with-Reason, does not work in the Beta release 1 version.

- CSCea05360

  The Virtual Adapter in the Release 4.0 VPN Client does not appear in the Cisco SetMTU utility.

- CSCea07430

  The Release 4.0 VPN Client is launched and the splash screen appears briefly, but the VPN Client dialog doesn't appear for approximately one minute, along with the following error:

  > The necessary VPN sub-system is not available. You can not connect to the remote VPN server.

  Something has caused the VPN client service not to load.

- CSCea07466

  If logging is started from the command line application Ipseclog.exe, the VPN Client GUI does not display any events in its log. Do not start Ipseclog.exe in a separate window if you intend to use the VPN Client Graphical User Interface (GUI). Use Ipseclog.exe only when using the VPN Client command line (vpnclient.exe) option.

- CSCea10174

  Some of the VPN Client dialogs show a question mark (?) in the upper-right corner, which is usually an indication of context sensitive help using Windows Help. The VPN Client does not use Windows Help and therefore these question marks do not bring up any available help for that dialog.

- CSCea12268

  The Virtual Adapter keeps its interface data from the VPN connection even after it is disconnected. The interface is disabled correctly but the IP address, mask, DG, DNS and WINs are all visible by looking at the adapter properties. This data should be cleared out after disconnecting.

- CSCea13071

  On the VPN Client for Mac, the Release 4.0 VPN Client banner is smaller than the 3.x VPN Client banner and may not display your entire banner and your users may have to use the scroll bar to see the entire message.

- CSCea13395

  VPN Client connections using IPSec over TCP do not see the status bar update when the VPN Client attempts a connection to one of the configured backup servers.

  The user sees only the primary server when connecting. For example:

  Initializing TCP to xxx.xxx.xxx.xxx...

- CSCea14713

  If the Ethernet interface loses link during a VPN Client connection, the following bogus error message appears:

  > Secure VPN Connection terminated locally by the Client
  >
  > Reason: An unrecognized error occurred while establishing the VPN connection.

  This message should indicate you have lost a connection with the peer.

- CSCea18578

  When using Start before Logon and a connection entry with a Microsoft digital certificate, you see an error indicating the certificate cannot be used. After the error message occurs, the VPN Client still displays the button [Cancel Connect] instead of [Connect]. Simply choose another connection entry and click [Cancel Connect] to attempt another connection. In this state, the [Cancel Connect] button functions as if it were the [Connect] button.

- CSCea18601

  The Force Network Login feature (also known as Netlogin or Automatic logoff) does not currently display any events in the VPN Client Event log.

- CSCea19946

  The VPN Client Banner has a feature that will require the user to scroll down to read the entire banner before continuing. This happens only if the Banner has a lot of text and is many lines long. On slower PCs, this feature does not work in some cases, and they can to continue connecting without reading all the banner text.

- CSCea20120

  Using Start before Logon, if you press ENTER to try to connect, depending on what TAB you left the VPN Client in last time, it either does nothing or shows a Cert View for one of your Certificates. You must click Connect to establish a VPN connection.

- CSCea22221

  The VPN Client does not add the Loopback address (127.0.0.1) to ZoneAlarm or ZoneAlarm Pro's Trusted Zone.

- CSCea22491

  The VPN Client for Mac, Release 4.0 Beta 2, does not work on a system running OS X 10.1.5.

  The Beta 2 VPN Client connects properly only on workstations with OS X 10.2.x.

- CSCea23182

  On Windows 2000 and/or Windows XP if the VPN Client loses its connection or fails to connect it might leave the virtual adapter enabled and cause network connectivity problems.

After losing the client connection or failing to connect the PC cannot communicate on the network. The output of an ipconfig /all command shows the virtual adapter as one of the PC's active interfaces.

- CSCea24882

  After connecting and disconnecting multiple times, the ability to connect might be lost, and the following error might occur on a Windows NT 4.0 SP6 system:

  "The necessary VPN sub-system is not available. You can not connect to the remote VPN server."

- CSCea35228

  High levels of VPN Client log activity might cause periods of sluggish client performance. This is most likely to happen when log levels are set to 3-HIGH and many events are being generated. An example would be having all event classes set to 3-HIGH, and while connecting, the large amount of IKE events may cause the VPN Client to "hang" for a period of time.

- CSCea35592

  The VPN Client event log displays the following events on Windows 2000 and/or Windows XP systems:

  76 14:14:51.082 03/04/03 Sev=Warning/2CVPND/0xA3400011

  Could not find (null) in IpHlpApi.DLL

  These events will only appear on operating systems that use the Virtual Adapter (Windows 2000 and Windows XP).

- CSCea38204

  When connecting the Release 4.0 Cisco VPN Client to an IOS VPN gateway, the VPN Client might initiate multiple IKE rekeys and then disconnect.

- CSCea38022

  Upgrading the Release 4.0 VPN Client using InstallShield on a Windows NT system might result in the VPN Client failing to connect. If the connection fails, the VPN Client displays the following event message:

  1 11:29:16.928 03/06/03 Sev=Critical/1CM/0xE3100004

  Failed to initialize the ipsec driver! Returned 1

  The problem is that the VPN Client's IPSec driver is not installed correctly.

This problem occurs only after an upgrade with InstallShield, not after a clean installation. This problem should not be an issue when using the VPN Client's MSI-based install. If you encounter this problem, uninstall the VPN Client, reboot the PC, then the reinstall the VPN Client.

- CSCea38311

  When the Release 4.0 VPN Concentrator is configured to send Alerts (Delete with Reason (DWR) messages) and the Release 4.0 VPN Client is configured to Auto Initiate, the Client does not suppress DWR messages and the user must click OK to clear the message to allow Auto Initiation to continue. This behavior is different from the Release 3.6 VPN Client, which does not display disconnect messages when Auto Initiation is in use.

  This occurs only when using a Release 4.0 VPN Concentrator and a Release 4.0 VPN Client.

Documentation Change

In the *VPN Client Administrator Guide, Release 4.0*, on page 2-7, in Table 2-1, "vpnclient.ini file parameters," make the following change to the information in the Values column for the OutlookNotify parameter. This parameter controls Microsoft Outlook to Microsoft Exchange polling behavior:

0 = Enable (Default)—Outlook polls every minute for new mail notifications. This might cause Outlook Folder Synchronization issues. The default state, if OutlookNotify is not present in the vpnclient.ini file, is Enable.

1 = Disable—Prevent the VPN Client from forcing Outlook to poll for new mail, thus avoiding the synchronization process. In this case, new mail is detected only on a background 30 minute polling cycle, or when the user initiates a manual send/receive or switches between folders.

Documentation Updates

These Release Notes are the only documentation for Release 4.0.3. They cover Release 4.0, Release 4.0.1, Release 4.0.2.x, as well as Release 4.0.3. The following VPN Client documentation has been updated for Release 4.0. These documents contain information for all platforms on which the VPN Client runs:

- *VPN Client Administrator Guide, Release 4.0*
- *VPN Client User Guide for Windows, Release 4.0*

The most recent information specifically for the VPN Client for Linux, Solaris, and Mac OS X is in the following document, which was not updated for Release 4.0:

- *Cisco VPN Client User Guide for Mac OS X*
- *Cisco VPN Client User Guide for Linux and Solaris*

Documentation Correction

In *VPN Client User Guide for Windows, Release 4.0*, in the section "Removing a VPN Client Version Installed with MSI Installer," (page 2-8 in the hard-copy edition), in Steps 4 and 5, remove Figures 2-8 and 2-9 and the text references to these figures. These dialog boxes do not appear when unstalling the VPN Client using the MSI Installer.

Related Documentation

- *VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.0*
- *VPN 3000 Series Concentrator Reference Volume II: Administration and Management, Release 4.0*
- *VPN 3000 Series Concentrator Getting Started, Release 4.0*

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.